Universitat Autònoma
de Barcelona

ipGUI: Gestió web d'un servidor firewall sota GNU/Linux

Memòria del projecte

d'Enginyeria Tècnica en

Informàtica de Sistemes

realitzat per

Robert Vall i Mas

i dirigit per

Marc Talló i Sendra

Escola d'Enginyeria

Sabadell, *febrer* de *2010*

El sotasignat, Marc Talló i Sendra,

professor de l'Escola d’Enginyeria de la UAB,

CERTIFICA:

Que el treball al que correspon la present memòria
ha estat realitzat sota la seva direcció
per en Robert Vall i Mas.

I per a què consti firma la present.
Sabadell, febrer de 2010

Signat: Marc Talló i Sendra

Resum

Aquest projecte pretén ser una eina de gestió remota per a un servidor *firewall*, i un dels seus objectius bàsics és de que sigui una eina de fàcil utilització, útil i còmode, però alhora potent i altament configurable. Per a fer això, s'ha pensat que la millor manera era que es fes utilitzant una interfície web pels nombrosos avantatges que suposa, com ara per la seva fàcil administració remota, per la seva comoditat utilitzant tant sols un navegador, com també per exemple que no es necessita fer cap instal·lació a cap màquina remota perquè s'entén que gairebé tots els sistemes operatius moderns amb interfície gràfica, disposen de navegador.

L'àmbit apropiat per al servidor *firewall* de les característiques d'aquest projecte, podria ser per exemple els d'unes oficines, o una escola mitjana. És així perquè està pensat per a fer de pont entre dues xarxes, i per tant, tot el tràfic ha de passa per ell. En infraestructures de xarxa molt grans i de molt tràfic, els *firewalls* no estan en servidors, sinó en dispositius físics construïts especialment per a aquesta finalitat o integrats en els mateixos dispositius de xarxa (per exemple routers).

La aplicació en si, el què fa és interactuar entre el navegador de l'usuari i el *firewall* del sistema operatiu del servidor. Moltes vegades, gestionar un *firewall* resulta complicat, ja sigui perquè es necessiten forces coneixements tècnics, o perquè té una interfície no gaire amigable i complicada. Com s'ha comentat, el projecte intenta fer que un usuari sense gaires coneixements tècnics, pugui aplicar regles al *firewall*, i fer-ho a partir d'un navegador web, on hi ha formularis amb ajuda i altres eines d'interès.

El nom de l'aplicació precisament ve donat per aquestes característiques, ipGUI prové de *iptables Graphic User Interface*, és a dir, una interfície gràfica per l'iptables, que és el *firewall* nadiu en sistemes Linux.

Índex

Índex de figures

1 Introducció

Des de gairebé els orígens de les computadores, va esdevenir necessària la comunicació entre diferents màquines, permetent així molta més complexitat i donar més possibilitats. Va ser llavors quan es va començar a treballar en com permetre aquesta comunicació. Això va donar pas a la creació de les xarxes informàtiques, que són un conjunt de dispositius units entre si mitjançant cables, senyals, ones o altres mètodes de transport de dades.

Existeixen diferents tipus de xarxes (pública, privada, virtual, etcètera.) i protocols (AppleTalk, Frame Relay, Token Ring, etcètera). En l'àmbit de xarxes locals, des de fa anys un dels protocols més utilitzats a nivell mundial és l'Ethernet[1], que després a partir d'alguns dispositius es pot connectar a altres xarxes (Internet per exemple). En aquest projecte s'utilitza aquesta tecnologia.

Un concepte important a tenir en compte és el de tallafocs (*firewall* en anglès). És una eina que filtra el tràfic entre xarxes (mínim entre dues), i tant pot ser un dispositiu físic específic, com un software dins un sistema operatiu (com és el cas d'aquest projecte). Per entendre-ho millor, es podria veure com una caixa amb dos o més interfícies de xarxa en la què s'estableixen unes regles de filtratge amb el què es decideix si una connexió determinada que vol passar a través de la caixa pot establir-se o no, entre d'altres opcions.

Segons l'ús que se li vulgui donar al *firewall*, aquest pot estar connectat de diferents maneres a la xarxa. Per exemple, les més habituals serien entre una xarxa privada i Internet (per fer de mur entre l'exterior i l'interior) i entre dues xarxes privades (er separar dues xarxes i permetre o denegar certes connexions).

Altres àmbits on es podria aplicar ipGUI seria per exemple aïllar una xarxa de proves d'una en producció, per a formar part d'una zona DMZ, o també per a fragmentar una xarxa extensa. Per tant, no cal limitar el seu ús, i pot oferir servei a múltiples usos.

Per aquests motius, no és convenient veure un *firewall* només com a un control de seguretat, sinó que ofereix moltes possibilitats i és de molta ajuda als administradors de xarxes.

Actualment, en un entorn domèstic, habitualment s'utilitza un router ADSL per accedir a Internet, on aquest també fa funcions de *firewall*, sobretot per evitar algunes connexions des de fora a dins de la xarxa. Les opcions que presenten aquests routers però, no acostumen a tenir gaire marge de configuració, tot i que segurament en un entorn domèstic no fa falta. En un entorn

[1] http://ca.wikipedia.org/wiki/Ethernet

empresarial, sí que és bastant important poder tenir aquesta possibilitat de poder tenir un alt grau de configuració.

ipGUI significa ***ip****tables* ***G****raphic* ***U****ser* ***I****nterface*, on iptables és el *firewall*, això significa que el principal objectiu de l'aplicació és el de gestionar gràficament aquest *firewall*. I per a fer una aplicació més completa, s'afegiran funcionalitats interessants i útils.

Figura 1: Logo d'ipGUI

Les tecnologies utilitzades per a fer aquest projecte són vàries, però amb el fet comú que són programari lliure. El sistema operatiu del servidor és una Debian GNU/Linux estable 5.0 (Lenny), un servidor web Apache2, com a llenguatge de programació PHP, MySQL com a servidor de base de dades, i diverses aplicacions comunes en sistemes GNU/Linux.

L'estructura de la memòria és la següent. Aquesta és una petita introducció del projecte, seguit del seu estudi de viabilitat, i explicació d'alguns conceptes bàsics que cal tenir clars per entendre millor com funciona l'aplicació. A partir d'aquí, es passa a com es va començar a encarar aquest projecte, com es faria, els apartats que hauria de tenir, què es necessita, etcètera. Llavors es parla del disseny de l'aplicació, com hauria de funcionar, com s'hauria d'estructurar entre d'altres coses. En l'apartat d'implementació, s'explica més com s'ha instal·lat tot, les funcions, els arxius i carpetes que hi ha i coses semblants. Ja en els últims apartats, es parla dels problemes que hi ha hagut, les proves que s'han fet i les conclusions. I ja al final de tot, uns annexes que complementen la informació de la memòria, principalment manuals d'ajuda i imatges.

Pel què fa a com està organitzada la informació, cada apartat està degudament separat i numerat. Les imatges també estan enumerades i hi ha un índex en les primeres pàgines de la memòria. Altres característiques d'aquesta memòria són que en el text poden aparèixer referències numèriques a peus de pàgina, o que en les capçaleres de les pàgines a la dreta s'hi mostra l'apartat principal i a l'esquerra el sub-apartat.

Les motivacions principals que han portat a l'autor a fer aquest tipus de projecte són vàries, principalment les del seu interès per les xarxes, el poder aprofundir força el seu coneixement sobre la programació web, i també la de la seva predilecció per utilitzar programari lliure.

2 Estudi de viabilitat

2.1 Introducció

Aquest projecte pretén construir un sistema de control d'una xarxa privada a partir d'un servidor firewall, que pot controlar quines accions es permeten i quines no entre d'altres opcions, entre aquesta xarxa privada i l'exterior, entre dues xarxes, i altres estructures de xarxa diferents.

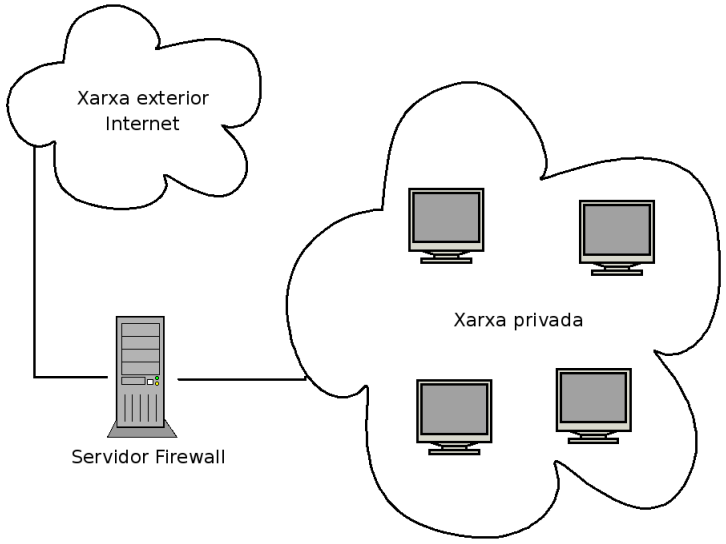

Figura 2: Possible diagrama de xarxa

2.1.1 Avantatges

Ajuda a tenir un major control de la xarxa, que en alguns casos és molt necessari. Fiquem per exemple una aula informàtica on s'està donant classe, i els alumnes s'estan connectant a Internet fent activitats que no tenen res a veure amb la classe. El professor, utilitzant aquesta aplicació, serà capaç d'evitar per exemple que cap màquina client de la xarxa es pugui connectar a Internet, com també especificar-ne una en concret, entre d'altres opcions.

Un altre cas podria ser el de voler fragmentar una xarxa, per dividir-la en seccions diferents, fent així disminuir el trànsit de paquets broadcast.

També podria ser que no es tingués accés directe a la màquina on hi ha el *firewall*. Es podria aplicar regles al tallafocs de manera remota, de la mateixa manera que si es tingués l'intèrpret de comendes i poder posar les regles necessàries.

Per a la gestió d'aquesta aplicació, no farà falta tenir grans coneixements informàtics, ja que es farà pensant en què per a l'usuari final que utilitzarà l'aplicació, sigui el més fàcil i entenedor possible. Per altra banda, també ha de permetre poder aplicar regles més complicades per a un altre tipus d'usuari més avançat. Per tant, s'haurà de combinar una interfície fàcil, amb una de més avançada. Això permet que l'aplicació pugui ser senzilla, i alhora molt completa per a usuaris avançats.

Aquest servidor, també es podria utilitzar per a altres funcions que es volguessin fer a posteriori. Per exemple, s'hi podria muntar un servidor de VPN[2] , utilitzar per desar-hi fitxers a compartir, i molts altres serveis. Així doncs no tindria una única funció i estalviaria haver de tenir altres servidors.

2.1.2 Inconvenients

Aquest projecte no avarca xarxes molt extenses, com podria ser per exemple tota una universitat, està pensat per a xarxes més petites.

Un dels altres inconvenients, és que aquest servidor el què fa és controlar el trànsit entre xarxes, però no el trànsit entre les màquines clients de dins la mateixa xarxa.

2.2 Objecte

2.2.1 Descripció de la situació a tractar

El sistema ha de ser capaç d'analitzar el trànsit de la xarxa que vol accedir a l'exterior, i aplicant les polítiques que hi ha en aquell moment, realitzar els accions necessàries.

Per fer-ho, s'utilitzarà una interfície gràfica per simplificar la seva configuració.

[2]Virtual private network - http://en.wikipedia.org/wiki/Virtual_private_network

2.2.2 Perfil de l'usuari

La persona que utilitzarà aquesta aplicació serà la persona encarregada de la xarxa. No ha de ser una persona amb gaires coneixements d'informàtics, per tant pot ser tant l'administrador de la xarxa com un professor.

També permetrà a un usuari avançat poder treballar tal com si tingués accés directe a la màquina.

2.2.3 Objectius

- Crear un servidor centralitzat.
- Crear interfície web de gestió del firewall, fent que la seva utilització sigui fàcil per a persones amb no alts coneixements informàtics.
- Crear interfície web de gestió del firewall, fent que un usuari avançat pugui aplicar regles més complicades.
- Facilitar la gestió de la xarxa de manera fàcil i intuïtiva.
- Crear un sistema d'autenticació perquè només l'administrador de la xarxa es pugui connectar a l'aplicació i gestionar-la.
- Utilitzar software lliure[3] tant per al sistema operatiu del servidor com per a l'aplicació.
- Estudiar els diferents sistemes operatius per a saber quin pot ser el més adient, així com també el llenguatge de programació de l'aplicació.

2.3 Descripció del sistema

2.3.1 Descripció general

El servidor, estarà dins la xarxa privada, i tot el trànsit que vulgui comunicar-se a l'exterior passarà per ell. Per a fer això, les màquines clients hauran d'estar configurades de tal manera que el servidor sigui la seva porta d'enllaç[4]. La xarxa també haurà d'estar configurada físicament perquè només sigui possible connectar-se a la xarxa exterior a través del servidor.

[3] http://ca.wikipedia.org/wiki/Programari_lliure
[4] http://en.wikipedia.org/wiki/Gateway_(telecommunications)

L'aplicació serà web, i es podrà gestionar remotament (autenticant-se prèviament). Aquesta aplicació el què farà serà comunicar-se amb el sistema operatiu per a què apliqui al seu firewall les polítiques que la persona que gestiona l'aplicació ha volgut.

2.3.2 Recursos

Els recursos de software del servidor, s'escolliran un cop finalitzat l'estudi de característiques que ha de tenir el servidor.

Hardware

Per aquest projecte no és necessari gaires recursos de hardware, solament el servidor.

El servidor ha de tenir unes característiques mínimes per a poder desenvolupar la seva funció de manera correcta. Encara que estigui pensat per a una xarxa de tamany reduït o mitjà, ha de tenir uns mínims. No és necessari per exemple que tingui un disc dur molt gran, ni una targeta gràfica bona. Per a fer de servidor firewall és millor que tingui una memòria RAM ràpida i un bon processador.

La creació de la xarxa i de les màquines clients no entra en aquest projecte, però la xarxa ha d'existir i les màquines clients han de tenir targeta de xarxa ethernet per a poder-se comunicar.

Recursos humans

Els recursos humans que ha de tenir aquest projecte són principalment:

- Cap de projecte
- Administrador de sistemes
- Programador
- Beta tester (equip de proves)

L'administrador de sistemes i el programador (poden ser la mateixa persona), seran els encarregats de crear i configurar el servidor així com també l'aplicació web.

El cap de projecte anirà fent periòdiques revisions al projecte. I el beta tester (preferiblement persona/es aliena/es al projecte), faran proves al sistema per veure si hi ha errors a corregir o suggerir quelcom.

2.3.3 Anàlisi cost - benefici

Material

Els costos materials directes d'aquest projecte són principalment el cost del servidor.

Els costos materials indirectes són els costos materials que serviran per crear el projecte, com ara el què utilitzaran l'administrador del sistema i programador.

Recurs	**Cost**
Servidor	1.500€
Sistema Operatiu	0€
Software	0€
Amortització PC's desenvolupament	200€
Total	**1.700€**

Taula 1: Costos materials

Personal

El sou dels diferents participants en el projecte és:

Recurs	**Preu per hora**
Cap de projecte	25€
Administrador de sistemes	20€
Programador	18€
Beta tester	10€

Taula 2: Sous

I els costos en les diferents etapes del projecte:

Tasca	**Hores**	**Cost**
Estudi de viabilitat	20h	500€
Estudi característiques servidor	30h	600€
Instal·lació i configuració bàsica del sistema operatiu al servidor	15h	300€
Disseny de l'aplicació web	15h	270€
Desenvolupament de l'aplicació web	120h	2.160€
Proves	8h	80€
Instal·lació del servidor a la xarxa	4h	80€
Proves finals	4h	80€
Documentació	20h	360€
Supervisió del projecte	15h	375€
Total	**251h**	**4.805€**

Taula 3: Costos personal

2.3.4 Pressupost

Pressupost del projecte:

Aspecte	**Preu**
Servidor	1.800€
Desenvolupament de l'aplicació i documentació	5.814€
Instal·lació del servidor a la xarxa	192€
Total	7.806€

Taula 4: Pressupost

Amb IVA, el pressupost total és de **9.054'96€**

2.3.5 Alternatives

Hi ha software existent semblant al què es vol crear. Però no s'en ha trobat cap que sigui adequat, ja sigui perquè era molt complicat, massa senzill, o perquè pel què era tenia un preu massa elevat. En general, poc personalitzat.

El què no es descarta és adoptar algunes característiques que es creguin adequades d'aquestes aplicacions.

Algunes d'aquestes alternatives són:

- Firewall Admin
- FirewallBuilder
- Bifrost

2.3.6 Avaluació de riscos

La majoria de possibles riscos que pot sofrir el sistema, són externs al projecte, és a dir, com ara que la xarxa no funcioni i no es pugui accedir a l'aplicació.

El risc principal és la fallada del servidor, en què cap màquina client de la xarxa privada es podria connectar a l'exterior. En aquest cas, només caldria connectar el cable de xarxa externa que està connectada al servidor, i connectar-se al switch/hub de la xarxa interna.

2.3.7 Organització del projecte

Aquesta és la metodologia de desenvolupament:

1. Estudiar diferents sistemes operatius i les seves propietats, i buscar quin pot ser el millor per a aquest servidor.
2. Estudiar les opcions que hi ha pel què fa als llenguatges de programació per a l'aplicació web.
3. Documentar-se del funcionament del firewall i de com es pot comunicar amb l'aplicació web.
4. Estudiar amb molt detall les opcions que ha de tenir l'aplicació.
5. Instal·lar el sistema operatiu al servidor.
6. Desenvolupar l'aplicació.

El projecte seguirà un model lineal de desenvolupament, tot i que es té previst que hi pugui haver petites modificacions durant el procés.

2.4 Planificació del Projecte

Es té previst que es comenci a preparar el projecte el dia 09 de Novembre de 2009, un cop aprovat l'estudi de viabilitat. A partir d'aquí, s'anirà desenvolupant el projecte, per a fer una entrega definitiva el mes de Febrer de 2010. En els dies posteriors s'entregarà la documentació pertinent.

Si per causes extraordinàries no es pogués entregar en aquestes dates, es faria el mes de Juny del mateix any.

Es calcula una planificació de 236 hores, amb les següents tasques:

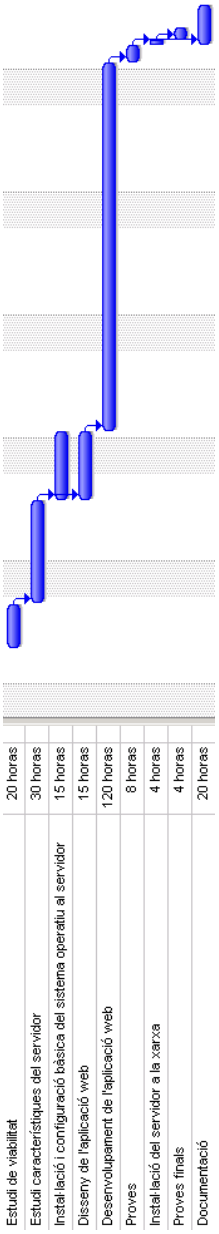

Figura 3: Tasques i diagrama de Gantt

2.5 Conclusions

Aquest projecte pot portar molts beneficis a certs àmbits, i ajudar molt en l'administració d'una xarxa.

El projecte no és específic ni molt encaminat per a un lloc determinat, és a dir, pot servir per a molt diferents llocs, sent fàcilment exportable. Amb el projecte finalitzat, es pot aplicar a un altre lloc fent només la instal·lació al servidor del sistema operatiu, configurar l'aplicació i configurar la nova xarxa, sent unes feines de poques hores.

No és un projecte excessivament car i és fàcilment exportable. Pràcticament no té inconvenients, i les poques probabilitats de risc que hi ha, no són gaire importants i poden fàcilment i ràpida resoltes. Per aquest fet, es creu que aquest projecte és viable.

3 Fonaments teòrics

La utilitat principal de l'aplicació, és la de gestionar un tallafocs (*firewall* en anglès) que està al servidor. Més concretament, el què fa és de pont entre l'usuari i la complexe configuració del tallafocs, fent més fàcil la seva gestió i aportant altres funcionalitats extres. El *firewall* que gestiona ipGUI és iptables, per tant, és important conèixer com funciona.

3.1 Què és un *firewall*?

És un dispositiu que filtra el tràfic entre xarxes (mínim entre dues), i tant pot ser un dispositiu físic específic, com un software dins un sistema operatiu (com és aquest cas). Com s'ha comentat en la introducció, es podria veure com una caixa amb dues o més interfícies de xarxa en la què s'estableixen unes regles de filtratge amb el què es decideix si una connexió determinada que vol passar a través de la caixa pot establir-se o no, però també s'hi poden aplicar moltes altres opcions.

Generalment, els *firewalls* a grans trets actuen d'una manera similar. Són un conjunt de regles en les què s'examina el trànsit de xarxa, i depenent d'això es fa una cosa o una altra (segons el tipus de paquet que sigui, s'apliquen unes regles o unes altres). Acostuma a haver-hi una política per defecte segons aquests tipus, i unes regles les quals s'aniran aplicant o no. Per exemple, es podria pensar en una política per defecte de denegar-ho tot, per després aplicar unes regles i deixar passar només el què es vol. Contràriament, també es pot ser més permissiu, i tenir una política per defecte d'acceptar-ho tot, però denegar coses concretes.

També resulta important l'ordre en què estan aplicades aquestes regles, ja que si per exemple hi ha dues regles contradictòries, s'aplicarà la què primer es trobi segons l'ordre de prioritat. En el cas de no trobar cap regla en la llista, al paquet se li aplicarà la política per defecte. Un exemple:

Configuració del *firewall*, apartat dels paquets que van destinats a la mateixa màquina:

1. Política per defecte: ACCEPTAR
2. DENEGAR totes les connexions que vagin al port 80
3. DENEGAR tot el què vingui de la màquina 192.168.0.10

4. DENEGAR tot el què vingui de la màquina 192.168.0.10 5.

Si per exemple arriba un paquet de 192.168.0.10 que va al port 22, passarà al punt (2) que l'acceptarà, en la següent regla (3) es denegarà el paquet ja que s'ha trobat una regla a aplicar, i ja no seguirà mirant les següents regles encara que siguin referents a paquets iguals.

Hi ha molts diferents *firewalls*, i com s'ha dit, el què utilitza aquesta aplicació és l'iptables, el qual ara se'n farà una breu explicació.

3.2 Què és iptables?

Iptables és l'eina que permet configurar les regles del sistema del filtrat de paquets IP del kernel de Linux, a partir de la branca 2.4 (a la 2.2 s'anomenava ipchains). Amb iptables es pot configurar un host per a què funcioni com un *firewall* adaptat segons les necessitats, a part de moltes coses més.

El seu funcionament és simple: A l'iptables se li passen unes regles, on s'especifica quines determinades característiques ha de complir un paquet, i quan s'acompleixi s'especifica una acció o target. Les regles tenen un ordre, i quan s'especifica o s'envia un paquet, es recorren en aquest ordre fins que s'acompleixen les condicions i s'aplica l'acció especificada o s'arriba al final de les regles i s'aplica la política per defecte. Per tant, l'ordre de les regles és molt important. En el diagrama de la figura 4 a la pàgina següent pot servir per fer-se una idea de quines accions realitza iptables quan rep un paquet per una interfície, però més endavant en aquest mateix apartat s'explicarà els components que formen aquest diagrama.

Aquestes accions es representen en el què s'anomenen targets, que indiquen el què s'ha de fer amb el paquet. Els més comuns són: ACCEPT, DROP i REJECT, però també n'hi han d'altres que permeten funcions a vegades interessants: LOG, MIRROR, ...

A continuació s'especificarà més com fucniona iptables. No cal entendre-ho tot fil per randa, l'important és treure'n una idea general de com funciona.

3.2.1 Com funciona?

El sistema de filtrat d'iptables es divideix en tres taules, cadascuna amb diferents "chains" o cadenes en les què pot concordar un paquet, i en cada cadena hi hauran unes regles.

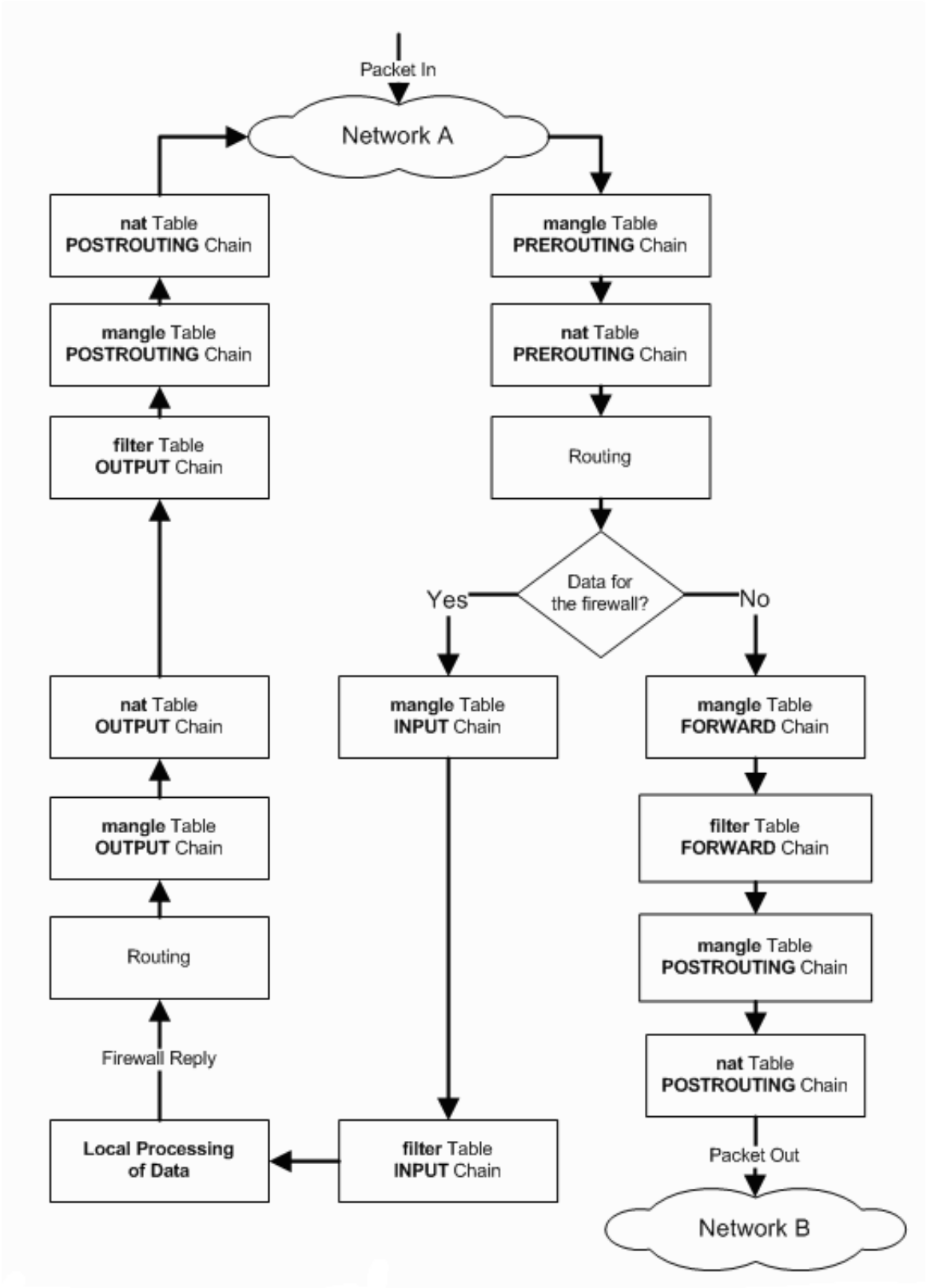

Figura 4: Diagrama de decisions

Quan un paquet concordi amb una "chain", es començarà a comparar amb les regles fins que alguna concordi segons l'ordre en què hagin estat introduïdes, i llavors se li aplicarà l'acció o "target" que s'especifiqui en la regla, com pot ser ACCEPT, DROP, QUEUE o RETURN.

Les taules en les què es basa iptables són tres, cadascuna amb les seves chains o cadenes:

Cadena filter: És la taula per defecte, ja siguin paquets amb destinació al servidor o per enrutar-los.

- INPUT: Controla tots el paquets que rep el servidor
- FORWARD: Controla el paquets que s'enruten des del servidor
- OUTPUT: Controla tots els paquets que surten del servidor

Cadena NAT: Aquesta fa referència a la modificació dels paquets que estan destinats a establir una nova connexió quan es creen.

- PREROUTING: Es modifiquen abans d'enrutar-los
- OUTPUT: Es modifiquen els paquets locals abans d'enrutar-los
- POSTROUTING: Es modifiquen després d'enrutar-los

Cadena mangle: Aquesta taula permet fer modificacions més especialitzades al tràfic que circula pel servidor. Permet fer balanceig de carrega per marcat IP, i altres funcionalitats avançades.

- PREROUTING: Modifica abans d'enrutar-los
- OUTPUT: Modifica els paquets locals abans d'enrutar-los

3.2.2 Creació de les regles

Amb iptables, es treballa a partir de comandes, seguint l'estructura "iptables [opcions]". Primerament se li ha d'indicar amb el modificador "-t" la taula des de la què es treballarà, ja que si no s'especifica per defecte es farà amb la filter. Per exemple "iptables -t nat", i a partir d'aquí ja es poden introduir les comandes per interactuar amb les taules.

El primer que s'ha de conèixer són les opcions que accepta iptables, que es poden dividir en diferents grups: comandes, paràmetres i les "match extenisions":

Comandes

Aquestes opcions especifiquen l'acció que s'ha de dur a terme. Només es pot fer servir una d'elles a la línia de comandes. A continuació les més importants:

- -A, –append chain rule-specification
  Afegeix al final d'una cadena la regla que s'especifica.

- -D, –delete chain rule-specification
  -D, –delete chain rulenum
  Elimina la regla de la cadena que concordi amb una especificació d'una regla o que estigui en la posició indicada de la cadena que se li passi.

- -I, –insert chain [rulenum] rule-specification
  Insereix una regla en la posició que se li especifica, si se li passa 1 com a numero de regla, la posarà en la primera posició, això ho farà també si no se li especifica cap "rule number".

- -R, –replace chain rulenum rule-specification
  Reemplaça una regla que es trobi en la cadena especificada, en la posició que se li indica per la especificació de regla que se li passa.

- -L, –list [chain]
  Mostra totes les regles en la cadena seleccionada, o si no se n'ha seleccionat cap, les mostra totes. Sempre de la taula que s'hagi especificat.

- -F, –flush [chain]
  Buida totes les regles de la cadena especificada, o totes les cadenes de la taula si no se'n especifica una. És el mateix que eliminar totes les regles una a una amb "-D".

- -P, –policy chain target
  Estableix la política per defecte per a la cadena donada. És l'acció que s'efectuarà si no s'acompleix cap de les regles.

Paràmetres

Aquests paràmetres són el que configuren l'especificació de la regla (es fan servir en les comandes append, insert, delete, replace). Les més importants:

- -p, –protocol [!] protocol

  El protocol a comprovar en el paquet. El protocol, pot ser tcp, udp, icmp o all. També pot ser un valor numèric segons l'arxiu "/etc/protocols". El símbol "!" inverteix la comprovació. El numero zero equival a tots els protocols i és l'opció que es pren per defecte quan s'omet aquesta opció.

- -s, –source [!] address[/mask]

  Adreça d'origen. L'adreça pot ser un nom d'una xarxa o d'un host (encara que posar un nom que necessiti d'una resolució externa com una consulta DNS normalment és una mala idea), una direcció IP d'una xarxa (amb mascara) o una direcció IP. La màscara pot estar tan en format IP, com en format curt, on es diu el nombre de bits que estan a 1 de la direcció IP, /24 == 255.255.255.0. L'us del símbol "!" inverteix el sentit de la comparació, per tant coincidirà qualsevol paquet amb origen diferent a l'especificat. També es pot fer servir l'alies src.

- -d, –destination [!] address[/mask]

  Adreça de destí. Funciona exactament igual a com ho fa la opció source. També es pot fer servir "–dst".

- -j, –jump target

  Aquesta opció especifica quina acció s'ha de prendre en cas de que el paquet coincideixi amb la regla.

- -i, –in-interface [!] name

  Nom de la interfície per on ha entrat el paquet (només vàlida per als paquets que entrin a les cadenes INPUT, FORWARD i PREROUTING. Si s'especifica "!" s'inverteix l'efecte. Si s'omet la opció concorda amb qualsevol interfície.

- -o, –out-interface [!] name

  Nom de la interfície per la que sortirà el paquet (només per les cadenes FORWARD, OUTPUT i POSTROUTING). El símbol "!" inverteix la selecció i si no se n'especifica cap hi concorden tots.

Match extensions

Iptables pot executar paràmetres estesos per comprovar els paquets. D'alguna manera són més punts de comparació que permeten afegir complexitat a una regla, amb altres paràmetres que depenen del protocol que es vulgui filtrar, l'estat del paquet, la mida, la MAC, etc. Això és conegut amb el nom de "Match Extensions".

Aquestes es carreguen de dues maneres diferents: de forma implícita quan s'afegeix "-p" o "–protocol" segons el protocol especificat, o amb el paràmetre "-m" o "–match" seguit pel nom del "matching module", després d'això es podran fer servir varies opcions de línia de comandes més. Es pot fer servir la opció "-h" o "–help" per obtenir informació especifica sobre el "matching module" que s'especifica. L'ús del símbol "!" és pot fer servir en la majoria d'opcions.

Altres opcions

- -v, –verbose
  Afegeix més detalls a la sortida de les comandes.
- -n, –numeric
  Força mostrar les direccions IP, números de port, etcètera, de forma numèrica en comptes de mostrar noms de màquina, noms de servei, etc.

3.3 Altres conceptes importants

En aquesta memòria es parlarà de molts conceptes tècnics. Normalment se'n fa una referència amb un link informatiu, o s'explica una mica. Ara s'explicaràn els més importants perquè quedin clars des del principi.

- PHP: És un llenguatge de programació interpretat utilitzat per generar pàgines web dinàmiques. Significa que a l'usuari se li mostra només la sortida, però que el què s'ha mostrat s'ha executat al servidor. Això permet realitzar operacions molt més complexes que no pas amb HTML sol.
- Servidor: És una computadora que sol tenir unes característiques hardware diferents a les domèstiques, com ara molta capacitat de processament, i molta i ràpida memòria. Aquests

poden tenir diferents finalitats , o també poden tenir molts usos en un sol servidor, però acostumen a oferir serveis a altres màquines, com ara un servidor web on hi ha pàgines web, un servidor de fitxers on es poden desar dades, o un servidor *firewall* com és aquest cas.

- Adreça IP: És un número que identifica d'una manera lògica un dispositiu en una xarxa. Serveix per diferencia'l i per tant, no hauria d'estar repetit dins d'una xarxa (xarxa privada, Internet, etcètera).

- Comanda: És una instrucció o ordre que un usuari li dona a un sistema usualment per a rebre una resposta o obtenir un comportament determinat. Hi pot haver el cas que el mateix sistema dongui una ordre al mateix sistema.

- Login/logueig: Té el mateix significat que "autenticació" però sovint enfocat a la informàtica. Quan es diu que una persona es logueja en un lloc, vol dir que ha entrat alguna espècie de nom d'usuari i/o contrasenya per accedir a un lloc restringit. Desloguejar, significa el contrari, que s'ha sortir del lloc restringit.

- Servei: Vindria a ser un programa informàtic que resta pendent d'oferir servei a altres màquines. Aquest pot ser de molts diferents tipus, com ara web, de fitxers, d'hora, de bases de dades i altres.

4 Anàlisi de l'aplicació

En aquest apartat d"'Anàlisi de l'aplicació", s'explicarà què ha de fer l'aplicació i com. Es planifica quines són les característiques principals que ha de tenir, i quins són els mitjans en què es pot desenvolupar.

4.1 Requisits funcionals

Aquí es farà una descripció del comportament desitjat del software. Després d'això i en els següents apartats, tenint en compte aquests requisits, es descriurà més concretament com s'ha fet l'aplicació.

A continuació, un llistat dels requeriments funcionals:

- Es vol desenvolupar una aplicació per a gestionar un *firewall*.
- L'aplicació ha de ser accessible remotament.
- Ha d'estar en un servidor.
- La manipulació de l'aplicació per part de l'usuari, ha de ser fàcil i intuïtiva, aportant també en tot moment la informació que es necessita, així com també un apartat d'ajuda.
- Els diferents apartats de l'aplicació, han d'estar separats degudament.
- Ha d'haver-hi un sistema d'autenticació amb usuari i paraula clau per a poder accedir a l'aplicació. Aquestes paraules clau, s'han de desar de manera encriptada al servidor.
- En el cas d'inactivitat per part de l'usuari, passat un temps determinat, aquest s'ha de desconnectar automàticament per seguretat.
- Hi ha d'haver diferents usuaris, no només un. Aquests es podran crear i esborrar.
- Hi ha d'haver dos tipus d'usuari, uns que siguin administradors i puguin fer canvis al sistema, i uns d'invitats, que només puguin observar sense poder fer cap canvi al sistema.
- Els usuaris han de poder canviar alguns aspectes del seu compte personal, com ara el nom i cognoms, correu electrònic de contacte, així com també la seva paraula clau.

- El sistema ha de poder permetre guardar la configuració del *firewall*, així com també carregar-la i esborrar-la.
- Hi ha d'haver la possibilitat de carregar una configuració determinada al iniciar el sistema, per si mai es para el servidor, que al carregar no s'hagi de tocar res i ja funcioni correctament el *firewall*.
- L'aplicació ha de fer de pont entre l'usuari i el *firewall* del sistema operatiu del servidor.
- L'aplicació ha de permetre fer ús de les característiques més importants del *firewall* a partir de formularis de fàcil comprensió.
- Aportar un assistent per a afegir les regles més comunes. És a dir, formularis que facin unes tasques concretes on només s'hagi de ficar com a molt un parell de dades, i es crei la regla desitjada sense haver de fer cap cosa complexa.
- En cas de necessitar alguna característica molt complexa del *firewall* i que amb l'aplicació no es pot arribar a fer, hi ha d'haver alguna manera de poder fer-ho.
- Hi ha d'haver un sistema de logueig, que enregistri quan un usuari entra, i els canvis que fa al sistema. Aquesta informació no ha de poder ser modificada per ningú, però sí mostrada a tothom.
- El sistema ha de proveir diferents sistemes per a evitar errors i per seguretat. Per exemple, quan es crei un usuari s'ha de comprovar que no n'hi hagi un altre amb el mateix nom d'usuari, quan es canvii la paraula clau del compte personal s'ha de ficar l'anterior i ficar dos cops la nova, etcètera.
- Quan un usuari faci canvis al sistema (canvis en la configuració del *firewall*, usuaris afegits i borrats, modificacions dels comptes personals, ...), l'aplicació ha de mostrar informació a l'usuari per a que sàpiga que s'han realitzat aquestes tasques.
- Quan s'hagi de mostrar llistes llargues (com ara un llistat dels logins dels usuaris), s'hauran de mostrar de manera paginada, fent llistes d'entre 30 i 50 entrades i que es pugui anar canviant fàcilment a partir de botons.
- El sistema ha de detectar automàticament coses del sistema com ara les interfícies de xarxa que hi ha per exemple per a fer un menú desplegable, per evitar errors. Així si hi

ha canvis en el sistema (s'afegeix una nova interfície de xarxa per exemple), no s'haurà de fer cap canvi a l'aplicació.

- Com que l'aplicació ha de ser accessible remotament, en cas de fallida, s'ha de proveir d'una eina local (que es faci directament al servidor) que permeti fer un "reset" a les regles del *firewall* fàcilment, permetent fer només aquesta acció, i que es necessiti usuari i paraula clau.
- Ha d'haver-hi un apartat que mostri gràfiques d'estadístiques del servidor, com ara el tràfic de xarxa o l'estat de la memòria.
- El pressupost per a finançar aquest sistema és de 9.054'96€.

Més endavant, en les fases de disseny i implementació, es va pensar que es podria dotar d'altres característiques per fer que l'aplicació fos encara més completa. Per tant, a posteriori es van afegir altres requeriments funcionals:

- Mostrar estadístiques que pugin ser d'utilitat, com ara l'estat de la xarxa a certes hores o dies, o també la càrrega del servidor (memòria i altres).
- Dotar d'un sistema d'avisos. Que hi hagi un canal de comunicació entre els diferents usuaris de l'aplicació, que sigui senzilla i útil.
- Els avisos només els poden crear els administradors.
- D'avisos n'hi pot haver de diferents tipus, i quan es mostrin, s'ha de veure qui i quan s'ha creat.
- Els avisos s'han de poder borrar individualment. En aquest cas, també son els administradors els únics que poden borrar.

4.2 Requisits no funcionals

En aquest apartat es diu què necessita l'aplicació per funcionar, com ara quines característiques ha de tenir el servidor, què necessita el client, com ha d'estar la xarxa, etcètera.

4.2.1 Requisits hardware del servidor

Com que està pensat que aquesta aplicació esta dissenyada per a xarxes petites/mitjanes, el requisits de hardware del servidor no són molt elevats. Podria ser important tenir un bon processador i una memòria RAM ràpida.

El més important, és que ha de tenir un mínim de dues targetes de xarxa (més depenent d'on es col·loqui el servidor i la seva finalitat). Això és per a separar físicament les xarxes, ja que si no es fa així, el paquets podrien passar per un altre camí i saltar-se el *firewall*.

4.2.2 Requisits del navegador client

El navegador ha de complir un parell de coses bàsiques, però que són comunes en pràcticament tots els navegadors web actuals.

La principal és tenir activat el JavaScript[5], que és un llenguatge de programació, que és una cosa molt comuna dels navegadors. ipGUI no utilitza molt JavaScript, però sí en alguns casos concrets. Per exemple, en la configuració del navegador web IceWeasel[6] (és el nom que té el Firefox a Debian, canviat per tema de llicències):

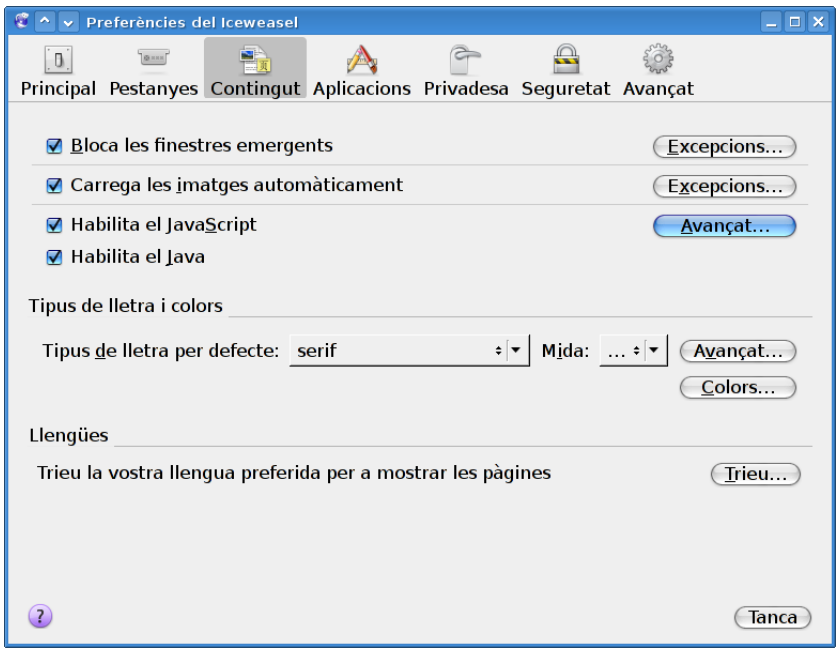

Figura 5: Preferències del navegador web IceWeasel

[5] http://ca.wikipedia.org/wiki/JavaScript
[6] http://ca.wikipedia.org/wiki/IceWeasel

Per a una millor visualització, l'aplicació hauria d'estar optimitzada per a una resolució de 1024x768 o superior.

L'aplicació també ha de ser compatible i visualitzar-se correctament amb la majoria de navegadors web més utilitzats, com pot ser Mozilla Firefox, Internet Explorer, Safari o Opera.

4.2.3 Estructura de la xarxa

Evidentment un servidor *firewall* sense estar connectat a una xarxa, no serveix de gaire. És necessari tenir una xarxa i configurar-la degudament, però això dependrà de la utilitat que se li vulgui donar al *firewall*, on el lloc que ocuparà el servidor ipGUI serà un o un altre.

Per exemple, en un entorn domèstic o oficina petita on hi ha una xarxa privada i un punt d'accés a Internet, podria ser:

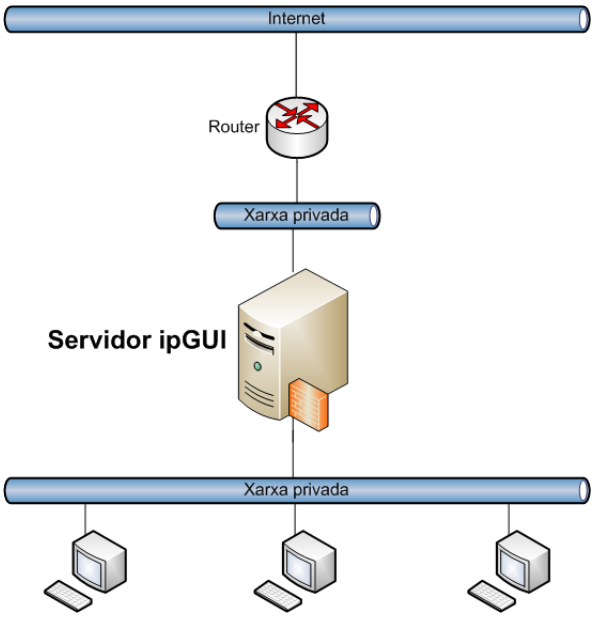

Figura 6: Esquema de xarxa 1: Una xarxa privada

En aquest cas per exemple, com que el servidor enruta el tràfic de la xarxa, s'ha de configurar a les màquines client que la la porta d'enllaç sigui el servidor.

Una altra funcionalitat que se li podria donar a ipGUI, és el de fraccionar una xarxa privada. És a dir, semblant a l'esquema anterior, però dividint la xarxa en dos o més subxarxes, per protegir-se entre si, o per per disminuir el trànsit de broadcast per exemple. En aquest cas, l'estructura podria ser:

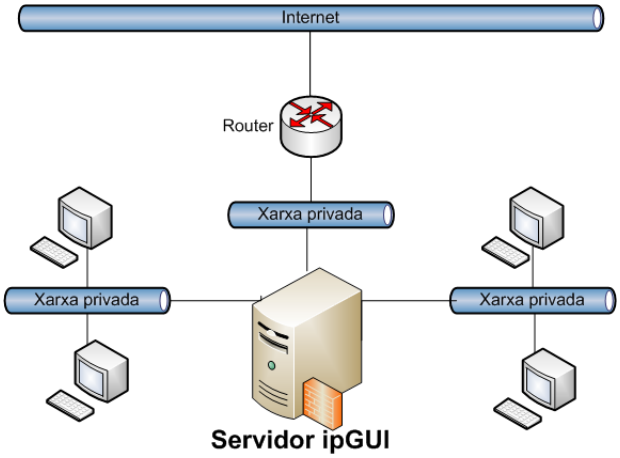

Figura 7: Esquema de xarxa 2: Fragmentar xarxa

Una altra utilitat més professional, podria ser la de tenir una zona DMZ[7]. Una zona DMZ, també anomenada zona desmilitaritzada, és una xarxa local (habitualment amb servidors) que està entre una xarxa interna i una xarxa externa (habitualment Internet). També pot ser que hi hagi més d'una zona DMZ a separar.

El seu ús més freqüent, és el de permetre que les connexions des de la xarxa interna i externa a dins la zona DMZ, però denegar les de la zona DMZ a la xarxa interna. Un exemple:

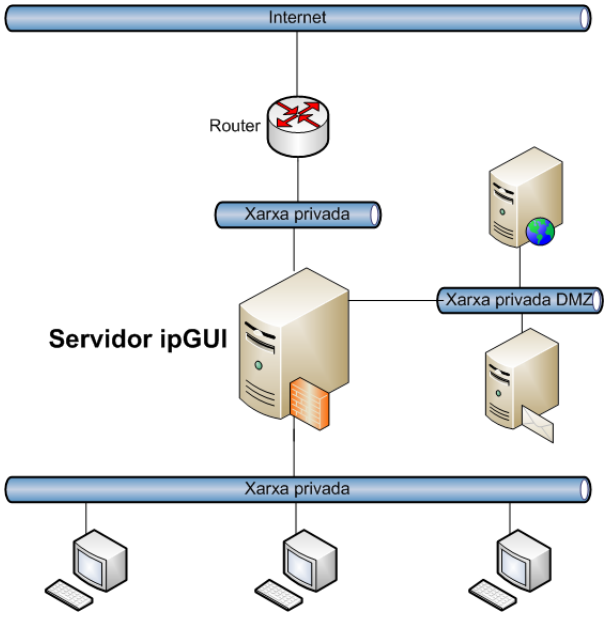

Figura 8: Esquema de xarxa 3: Zona DMZ

Hi ha altres estructures de xarxa on ipGUI pot fer unes funcions determinades. Fins hi tot, no es descarta ficar més d'un servidor ipGUI per a xarxes més complexes.

[7]http://en.wikipedia.org/wiki/DMZ_(computing)

4.3 Requisits tècnics

A continuació es comenta què hi ha fet de semblant, què s'ha triat per fer l'aplicació i el perquè.

4.3.1 Estat de l'art

A continuació, un llistat d'algunes aplicacions ja existents que són semblants a aquest projecte:

- Firewall Admin (http://firewalladmin.sourceforge.net): Una eina semblant a la què es vol crear. El què passa amb aquesta aplicació és que ja no es manté, des del 2005 que no s'actualitza ni es millora.

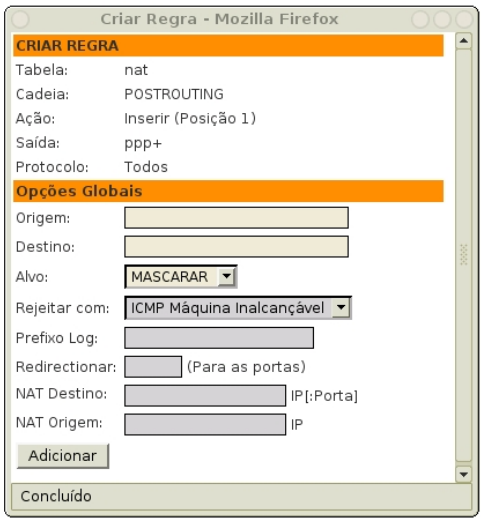

Figura 9: Firewall Admin

- FirewallBuilder (http://www.fwbuilder.org): Aquesta no seria una aplicació molt semblant, però la finalitat sí que és semblant. El què fa FirewallBuilder és a partir de la seva aplicació que s'instal·la al sistema (sota GNU/Linux, MS Windows i Mac OS X), crea un arxiu de configuració que posteriorment es pot carregar.

  Es poden realitzar configuracions força completes i complexes, però no és gaire intuïtiu ni usable. A més, si s'han de fer canvis, resulta inadequat haver de crear primer l'arxiu de configuració, carrega'l al *firewall*, i després provar.

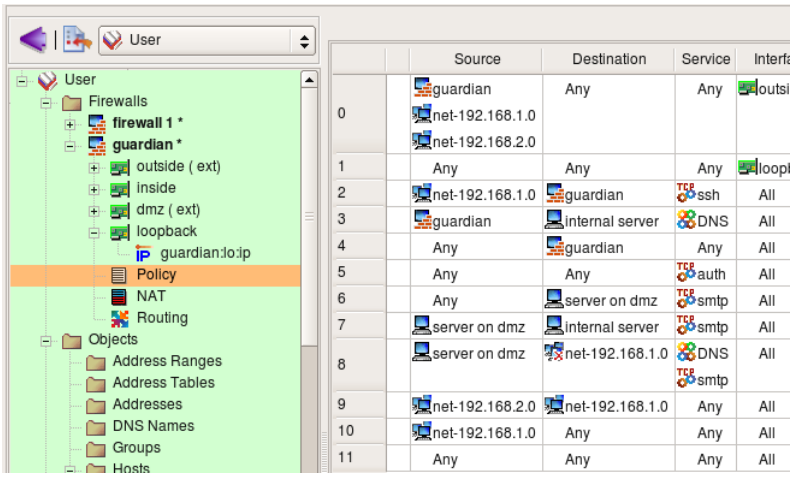

Figura 10: FirewallBuilder

- Bifrost (http://bifrost.heimdalls.com): Aplicació web feta amb Perl, que ofereix un seguit d'eines d'administració.

  És bastant bàsic, i a més per a poder tenir totes les funcionalitats, s'ha de pagar una llicència.

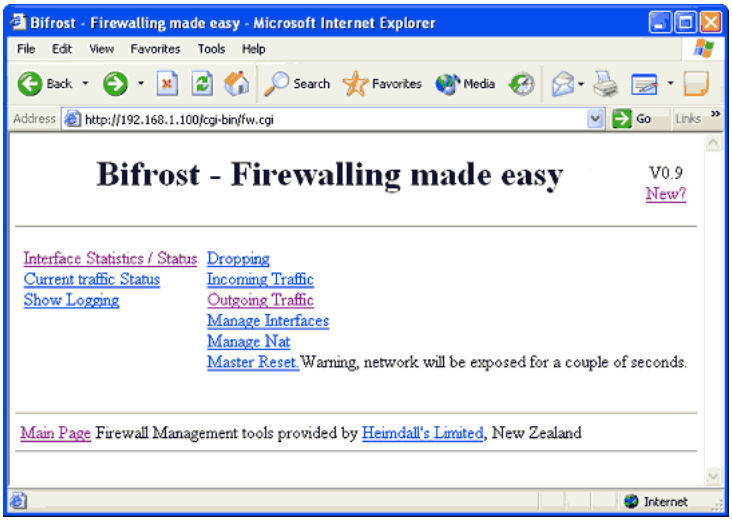

Figura 11: Bifrost

Es vol que ipGUI sigui una aplicació fàcil d'utilitzar, amb ajudes, completa, i amb eines complementàries. Aplicacions amb aquestes característiques pràcticament no n'hi ha, o són molt senzilles o massa complicades. El què es farà en aquest projecte, és pensar l'aplicació tal i com marquen els objectius, però tenint en compte aquestes aplicacions ja creades, ja sigui per evitar els seus errors com per veure coses positives en elles i adaptar-les al projecte.

4.3.2 Sistema operatiu

El sistema operatiu és bàsic, ja que determina molt com pot ser l'aplicació. Ha de ser un sistema estable i segur. Per aquests motius, com a sistema operatiu s'ha escollit una distribució GNU/Linux.

Abans de res, cal fer la diferenciació entre Linux[8] i GNU/Linux[9]. GNU/Linux és un sistema operatiu format per Linux, que és el nucli del sistema operatiu, i GNU[10], que són aplicacions lliures sota aquesta llicència. Anant per separat, un per si sol no serveix de gaire, Linux podríem dir que controla la màquina, la engega però no s'hi pot fer res, i les aplicacions, sense un lloc on es puguin executar tampoc serveixen de gaire.

S'ha optat per GNU/Linux per força motius, els principals i amb una breu descripció:

- Estabilitat i eficiència: Està pensat de manera molt modular, i fa que per exemple es puguin realitzar actualitzacions i canvis significatius en el sistema com podria ser canviar el motor del sistema operatiu (el nucli) sense cap problema.
  També és un dels sistemes que aprofita millor les característiques hardware.

- Seguretat: Es segueix la filosofia dels sistemes UNIX, i està basat en un robust sistema de permisos i usuaris. Això significa que un usuari pot modificar únicament els seus propis arxius (a no ser que el propietari n'hagi donat permisos). En això hi ha una excepció, que són els administradors, que poden modificar el sistema.
  A més, el fet que es pugui disposar del codi font del software, fa que qualsevol persona (per no dir milers de persones) ho pugui veure, trobar errors i millorar-ho.
  Algunes distribucions GNU/Linux, tenen diferents versions (per exemple l'estable i la de proves). Això fa possible que mentre es va treballant per fer el més segura la versió estable, es vagin fent proves per a la què serà la futura versió estable, sense comprometre la versió estable actual.

- Programari lliure: Això implica no només la gratuïtat del software, sinó també que Linux i les aplicacions GNU es poden modificar i que hi ha una gran quantitat d'aplicacions lliures de gran qualitat. Tot això amb una immensa documentació que es pot trobar lliurement, així com nombrosos grups d'ajuda a l'usuari.

[8] http://ca.wikipedia.org/wiki/Linux
[9] http://ca.wikipedia.org/wiki/GNU/Linux
[10] http://ca.wikipedia.org/wiki/GNU

Això fa possible també (i lligat amb la seguretat), que quan hi hagi actualitzacions de seguretat, es pugui gaudir ràpidament i lliure d'aquestes.

Dins de GNU/Linux, hi ha diverses distribucions, però s'ha escollit Debian[11] per a ser una de les més estables i segures, i es demostra sent una de les principals distribucions que utilitzen els servidors. La versió que s'ha instal·lat és una Debian GNU/Linux estable 5.0 (Lenny), que va esdevenir estable el 14 de febrer del 2009.

La versió del nucli (kernel) que incorpora aquesta versió estable de Debian és la 2.6.26-2-686.

Pel què fa a l'arquitectura del servidor, s'ha fet en un PC d'arquitectura x86[12], però com que el sistema operatiu GNU/Linux pot funcionar sobre altres arquitectures, aquesta aplicació pot funcionar sobre altres arquitectures. Aquesta compatibilitat varia segons la distribució, però concretament Debian, actualment té suport principalment per a Intel x86 / IA-32 ("i386"), Motorola 68k ("m68k"), Sun SPARC ("sparc"), Alpha ("alpha"), Motorola/IBM PowerPC ("powerpc"), ARM ("arm" and "armel"), MIPS CPUs ("mips" and "mipsel"), HP PA-RISC ("hppa"), IA-64 ("ia64"), S/390 ("s390"), AMD64 ("amd64").

4.3.3 iptables

El *firewall* que s'ha escollit ve determinat pel sistema operatiu escollit del servidor.

El *firewall* que tindrà el servidor, no és un servei que s'ha d'instalar a part, sinó que ja forma part del mateix nucli dels sistemes Linux. Aquest és iptables[13] (que s'anomena així a partir de la versió 2.4 del kernel de Linux, anteriorment s'anomenava ipchains), i és l'encarregat d'analitzar el trànsit IP, que a través de les seves eines/comandes es pot interactuar amb el nucli per gestionar la configuració del *firewall*.

Els paquets que circulen per la xarxa, poden ser de moltes maneres diferents, i són característics per exemple:

- Pels valors de les seves capçaleres (on es dirigeixen, d'on venen, número dels ports, ...)
- Segons el protocol (TCP, UDP, ICMP, ...)

[11] http://www.debian.org
[12] http://en.wikipedia.org/wiki/x86
[13] http://www.netfilter.org/projects/iptables/

- Broadcasts (multicast, dhcpdiscover, ...)
- Segons el contingut del paquet
- Característiques que no fan referència a un paquet en particular sinó amb la sumatòria d'aquests

Per tant, hi ha molts tipus de paquets diferents a la xarxa, i iptables és capaç de poder analitzar'ls, i a l'usuari de segons el seu interès, fer que el nucli pugi fer unes accions o altres, com per exemple, acceptar'ls, no permetre que passin (depenent d'on vinguin, d'on vagin, protocol, ...), modifica'ls, marcar'ls, i fer moltes altres coses. És un *firewall* molt complet, i treballant en el mateix nucli del sistema operatiu, el fa molt segur, estable i eficient.

La versió d'iptables que utilitza Debian en aquesta versió, és la 1.4.2.

4.3.4 Serveis i llenguatges

Tot el software del servidor, s'ha instal·lat a partir del programari que té Debian als seus repositoris estables. Això garanteix fiabilitat i seguretat en totes les seves aplicacions, així com també una manera ràpida i còmode d'aplicar actualitzacions de seguretat.

El servidor web escollit és un Apache2[14] (més concretament la versió 2.2.9). Es podria considerar el servidor web per excel·lència, no només per la seva gran acceptació (gairebé el 70% dels servidors web d'Internet l'utilitzen), sinó perquè des del seu naixement ha demostrat sobradament la seva estabilitat, solidesa i el seu alt rendiment respecte els seus competidors.

És veritat que per a aquesta aplicació poder no fa falta un servidor web tant complet, però es va pensar que per aprofitar el servidor ipGUI, podria allotjar altres serveis com ara servidor de fitxers, o altres. Així que l'Apache2, podria donar servei a altres utilitats. També s'ha escollit pensant amb nombrosa ajuda i documentació que es pot trobar, i que facilita el seu ús.

Com a llenguatge de programació, s'ha utilitzat PHP[15] 5.2.6. És ràpid, estable, i simple, és àmpliament suportat per Apache2, i ofereix moltes possibilitats per a treballar. És molt popular, i això ajuda en què hi hagi molta documentació. Un altre dels motius d'escollir PHP, i relacionat amb la simplicitat, és que permet creat aplicacions molt funcionals de manera relativament

[14] http://httpd.apache.org
[15] http://www.php.net

fàcil, i veient el temps del què es podia disposar per a fer aquest projecte, era bastant important d'utilitzar un llenguatge així de potent però fàcil d'implementar.

Als inicis del projecte es va plantejar si realment es necessitava o no l'ús d'un servei de bases de dades, ja que en principi només s'utilitzaria per a fer el login, i això es pot fer d'altres maneres (com per exemple utilitzant .htaccess[16] de l'Apache). També s'havia pensat que a l'aplicació només hi hauria eines de gestió del *firewall*. Posteriorment, es va pensar que a part de les funcionalitats a donar al *firewall*, també hi hauria altres eines per a fer una aplicació més completa, com ara mostrar estadístiques, gestió de diferents usuaris i tipus d'usuaris, mostrar les accions que desenvolupen els usuaris, manuals d'ajuda, i altres. Finalment, es va decidir ferne ús, i així donar totes aquestes funcionalitats extra, i també pensant que en futures versions segurament s'hauria d'utilitzar una base de dades.

S'ha utilitzat MySQL[17] 5.0.51, que és el complement ideal per a Apache2 i PHP5.

Per a fer certs scripts del sistema, s'ha utilitzat Bash[18], que està fortament arrelat als sistemes GNU/Linux. D'una manera molt senzilla i entenedora, es poden arribar a fer coses molt potents. La versió que ve per defecte amb aquesta versió de Debian estable és la 3.2.39.

4.3.5 Altres aplicacions

A part del software descrit en els apartats anteriors, l'aplicació web necessita algunes altres eines per al seu funcionament.

El servidor web Apache2, en el sistema s'executa com a usuari "www-data", i per a fer canvis a les regles de l'iptables, es necessita ser administrador del sistema (usuari "root" per exemple). Per tant, una aplicació web com és ipGUI allotjada en el servidor web, no pot fer canvis directament al *firewall* (per defecte www-data, l'usuari que executa l'Apache2, no és administrador). Per a casos similars, en què un usuari no administrador, necessiti executar algunes comandes concretes del sistema com a administrador, existeixen eines que fan de pont. L'utilitzat en aquest projecte és "sudo[19]" (de les sigles en anglès de ***super**user* -o ***s**ubstitute **u**ser-**do***).

[16] http://httpd.apache.org/docs/2.0/howto/htaccess.html
[17] http://www.mysql.com
[18] http://www.gnu.org/software/bash/bash.html
[19] http://ca.wikipedia.org/wiki/Sudo

El què fa aquesta eina és, a partir del seu fitxer de configuració (/etc/sudoers), dir quins usuaris poden executar certes eines d'administrador. Llavors l'únic que ha de fer l'usuari no administrador, és posar "sudo" davant de la comanda d'administrador que vol executar i ja està.

Alguna de les utilitats que té ipGUI per a facilitar-ne l'ús, és per exemple quan s'està entrant una nova regla, indica quines interfícies hi ha disponibles en un menú desplegable (tal i com mostra la figura 12), per no haver d'escriure-la a mà.

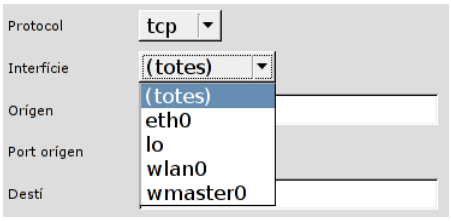

Figura 12: Menú desplegable de les interfícies

Per a saber les interfícies que hi ha, executa la comanda "ifconfig" (del paquet net-tools de Debian), que és una eina de configuració de la xarxa. Llavors, com que aquesta comanda també mostra molta altra informació, es necessiten altres comandes per a filtrar la informació desitjada, com és el cas de "awk[20]" (del paquet "gawk[21]" de Debian) o "grep".

Per a l'apartat d'estadístiques, s'ha utilitzat software extern de creació d'estadístiques, per després agafar els seus resultats i mostrar'ls a l'aplicació. Per a fer això s'ha utilitzat MRTG[22] i Munin[23].

Per a generar unes gràfiques que serveixen per a mesurar el trànsit que passa pel servidor, s'ha utilitzat Bwbar[24]. És només una eina perquè l'usuari pugui veure ràpidament si pel servidor hi està passant gaire trànsit.

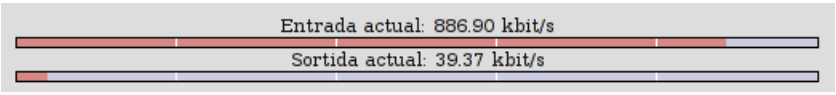

Figura 13: Bwbar

Altres comandes utilitzades, són per exemple "whoami" o "hostname", que són eines bàsiques en sistemes *NIX.

[20] http://cm.bell-labs.com/cm/cs/awkbook/index.html
[21] http://www.gnu.org/software/gawk/gawk.html
[22] http://oss.oetiker.ch/mrtg/
[23] http://munin.projects.linpro.no/
[24] http://www.kernel.org/bwbar.html

5 Disseny

Els primers sub-apartats fan referència principalment al disseny funcional, mentre que els dos últims al disseny gràfic d'ipGUI.

5.1 Casos d'ús

Els casos d'ús especifiquen el comportament desitjat d'un sistema, representant els requeriments funcionals. Descriuen què fa el sistema, no com ho fa.

A continuació es mostraran els casos d'ús d'aquesta aplicació.

Figura 14: Diagrama de casos d'ús

5.2 Base de dades

La complexitat de la base de dades de l'aplicació no és molt gran.

Com s'ha comentat en l'apartat 4.3.4 a la pàgina 40, quan es va començar a dissenyar l'aplicació, es va pensar que poder no feia falta ficar una base de dades perquè no calia, ja que per l'única cosa que poder feia falta és la d'autenticar usuaris, però això es pot far d'altres maneres. Finalment es va decidir que sí feia falta, per donar més funcionalitats extra com les que s'han acabat fent, i per si es vol seguir desenvolupant en un futur, doncs ja estar dissenyat des d'un principi per a treballar-hi.

Dins la base de dades "ipgui", hi ha les taules:

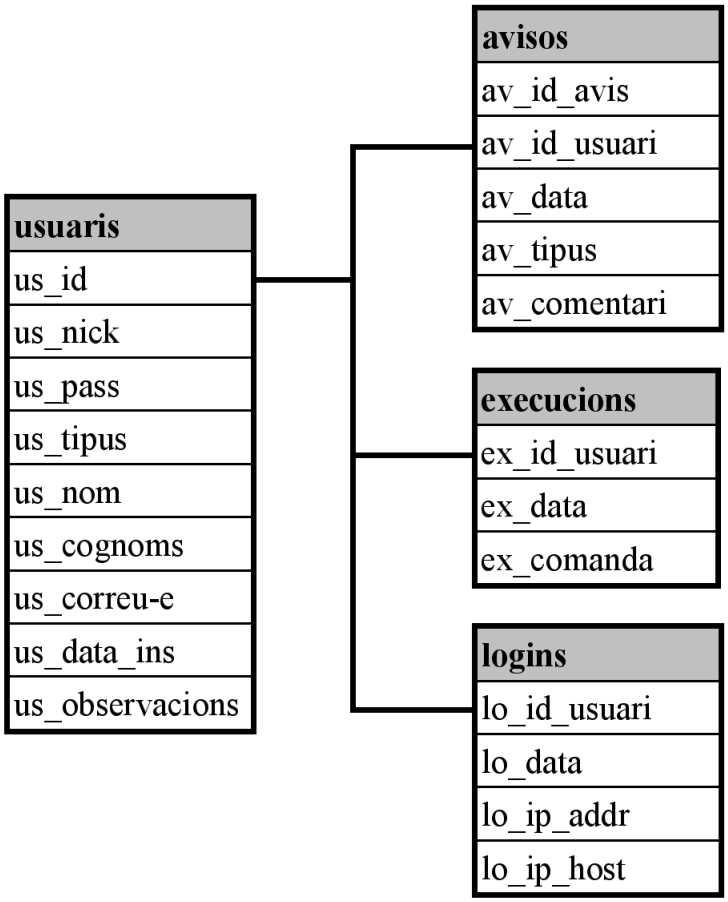

Figura 15: Taules de la base de dades

A continuació, la seva descripció:

Taula “usuaris”: És la taula on es desa la informació dels usuaris del sistema.

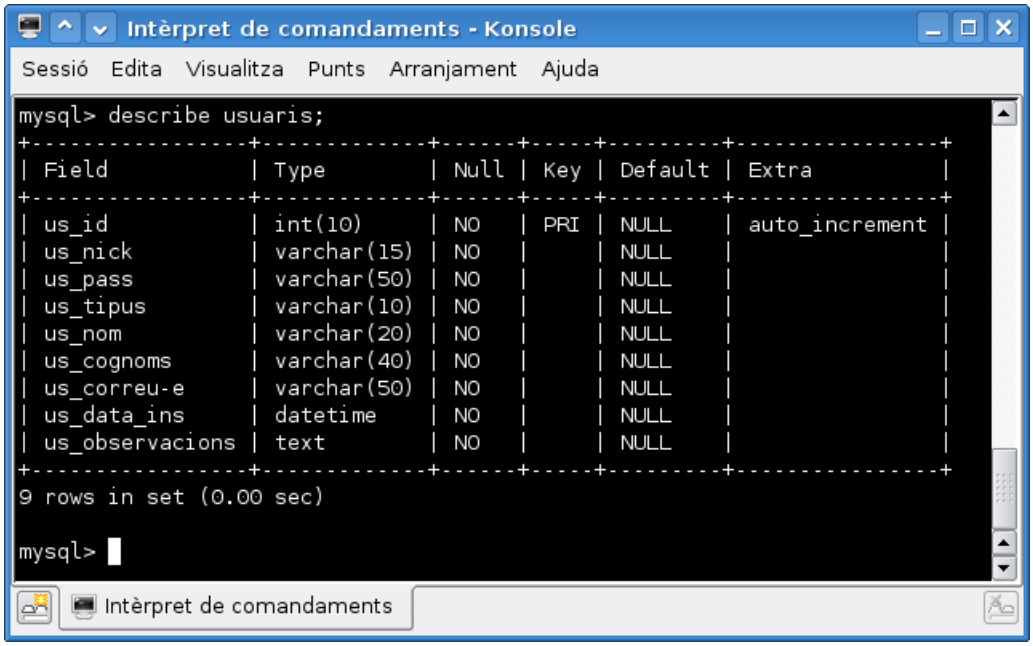

Figura 16: Taula “usuaris”

- us_id: El número d’identificació de l’usuari, cada usuari el té diferent
- us_nick: El nom d’usuari, el qual es fa servir per loguejar-se
- us_pass: El password de l’usuari encriptat sota MD5[25]
- us_tipus: Hi ha dos tipus d’usuari, administrador i visualitzador. Si és administrador, tindrà valor “admin”, si és visualitzador, hi haurà “viewer”
- us_nom: Nom de l’usuari
- us_cognoms: Cognoms de l’usuari
- us_correu-e: Correu electrònic de contacte
- us_data_ins: Data de quan va ser afegit
- us_observacions: Informació extra que es vulgui aportar

[25] http://ca.wikipedia.org/wiki/MD5

Taula “logins”: Informació referent a quan un usuari s’ha loguejat, i d’es d’on.

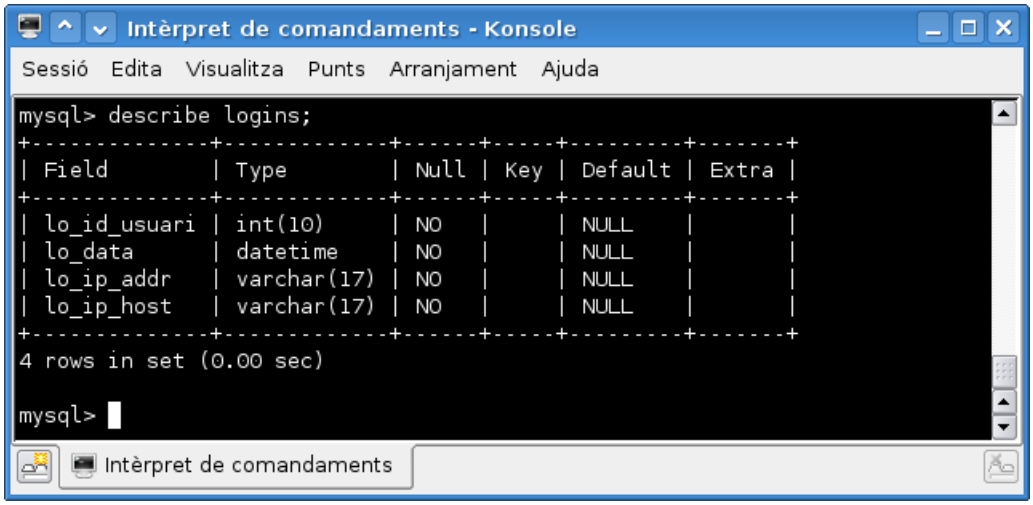

Figura 17: Taula “logins”

- lo_id_usuari: Número que identifica l’usuari
- lo_data: Data i hora de quan es va loguejar
- lo_ip_addr: IP des d’on es va connectar
- lo_ip_host: També la IP des d’on es va connectar, però pot ser que es connecti des d’una IP de dins un sistema de IP’s variables (comú en connexions ADSL). Moltes vegades pot coincidir amb “lo_ip_addr”.

Taula “execucions”: S’hi desen les accions que realitza cada usuari al *firewall*.

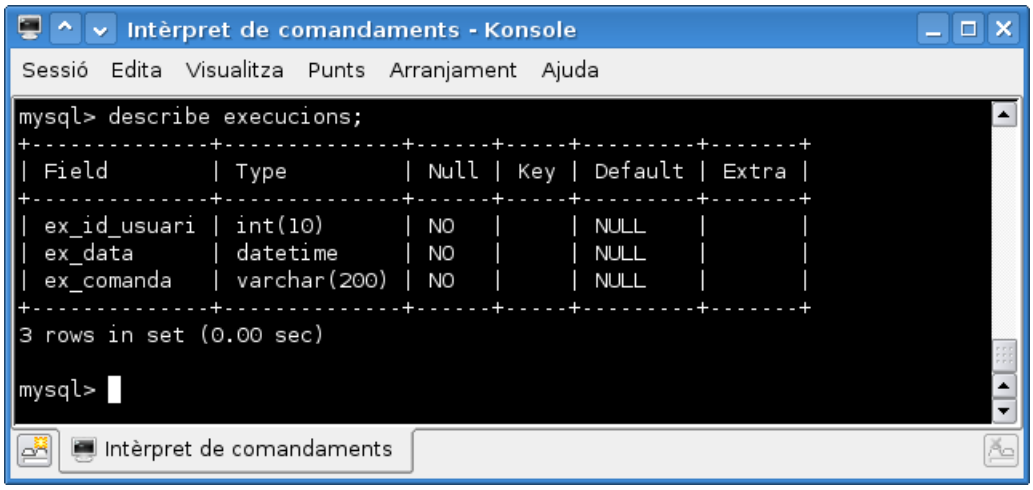

Figura 18: Taula “execucions”

- ex_id_usuari: Número que identifica l'usuari
- ex_data: Data i hora de quan va realitzar l'acció
- ex_comanda: Acció que va realitzar

Taula "avisos": Aquí si guarden les alertes, que serveixen per a donar a conèixer diferents esdeveniments als usuaris de l'aplicació.

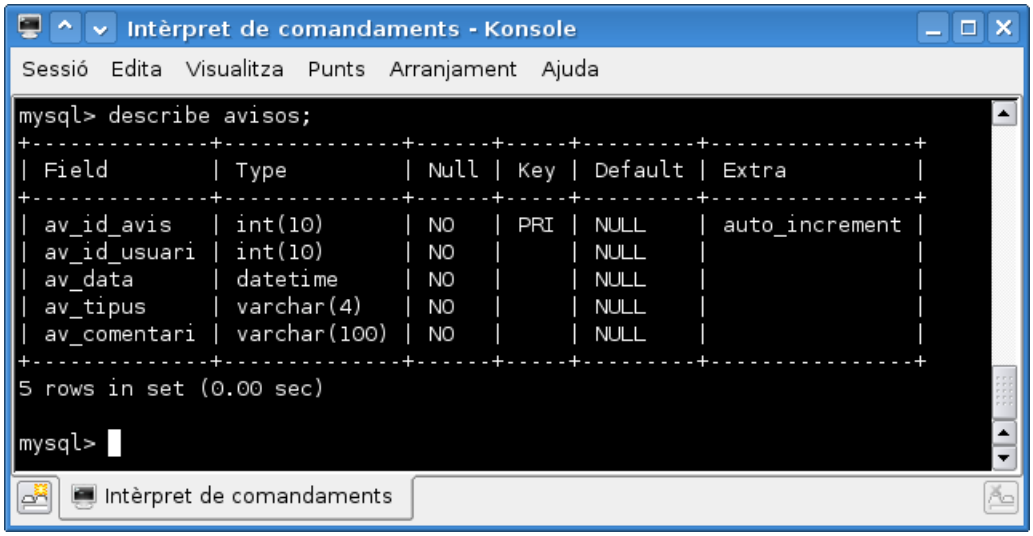

Figura 19: Taula "avisos"

- av_id_avis: Número que identifica l'avís
- av_id_usuari: Número que identifica l'usuari
- av_data: Data de quan s'ha creat l'avís
- av_tipus: Hi ha dos tipus d'avisos, els què són importants ("warn"), i els què són d'informació general ("info")
- av_comentari: Explicació de l'avís

Per a fer les crides a la base de dades sota PHP, en comptes d'utilitzar MySQL[26], s'ha utilitzat MySQLi[27]. S'ha utilitzat MySQLi (MySQL Improved) principalment per la seva seguretat, i perquè es recomana que s'utilitzi a partir de la versió 4.1.3 de servidor de MySQL. No canvia molt, però ofereix algunes funcionalitats extra interessants. A més, MySQLi pot aprofitar totes les millores de MySQL 5, tot i que en aquest projecte no ha fet falta utilitzar-ne.

Per a poder consultar les dades desades en aquestes taules, hi ha d'haver un usuari de MySQL que se li permeti. Com que no només ha de poder consultar, també se li han de donar permisos per a modificar, afegir, i esborrar. Per seguretat, el què no se li ha de permetre a aquest usuari són altres coses com ara, alterar l'estructura de les taules.

5.3 Estructura i funcionament de l'aplicació

A l'inici, hi ha d'haver un sistema d'autenticació d'usuari. I un cop autenticat, es portarà a la pàgina principal, i d'es d'aquí accedir a tots els apartats.

L'estructura de l'aplicació ha de ser àmpliament modular. I això significa diferents coses, les principals:

- Es separarà cada una de les funcionalitats principals de l'aplicació per mòduls . Per exemple, si hi ha un apartat que sigui el de crear regles, doncs hi haurà només una pàgina per a fer això on hi serà tot. També pot haver-hi mòduls dins d'altres mòduls, per a separar si cal els continguts.

- Hi haurà funcions que no seran exclusives en la seva tasca, principalment de dos tipus. El primer és el de funcions per a afegir codi PHP (arxiu "common.inc"), per exemple les capçaleres, i parts comunes de les pàgines. I l'altre el d'executar comandes al sistema per a interactuar amb el *firewall* (arxiu "commands.php"), ja que si per exemple s'han de crear regles, i hi ha diferents tipus de regles, amb una sola funció es puguin fer totes passant uns paràmetres o uns altres.

Cal tenir en compte que si un usuari no està autenticat, no ha de poder accedir a cap apartat. Això s'ha de controlar a l'inici de cada mòdul, comprovant si ho està o no, per evitar poder accedir-hi a partir de la URL[28]. També hi ha d'haver l'opció de desloguejar-se, sortint de l'aplicació.

[26] http://php.net/manual/en/book.mysql.php
[27] http://php.net/manual/en/book.mysqli.php
[28] http://en.wikipedia.org/wiki/Uniform_Resource_Locator

Com s'ha comentat en altres apartats, hi ha dos tipus d'usuari, un d'administrador i l'altre d'invitat. L'estructura de l'aplicació ha de permetre que segons això, automàticament es mostri o s'amaguin els apartats que comporten fer canvis en l'aplicació.

A continuació, es mostrarà com s'ha ordenat l'aplicació ens apartats i sub-apartats (depenent si l'usuari és administrador o invitat):

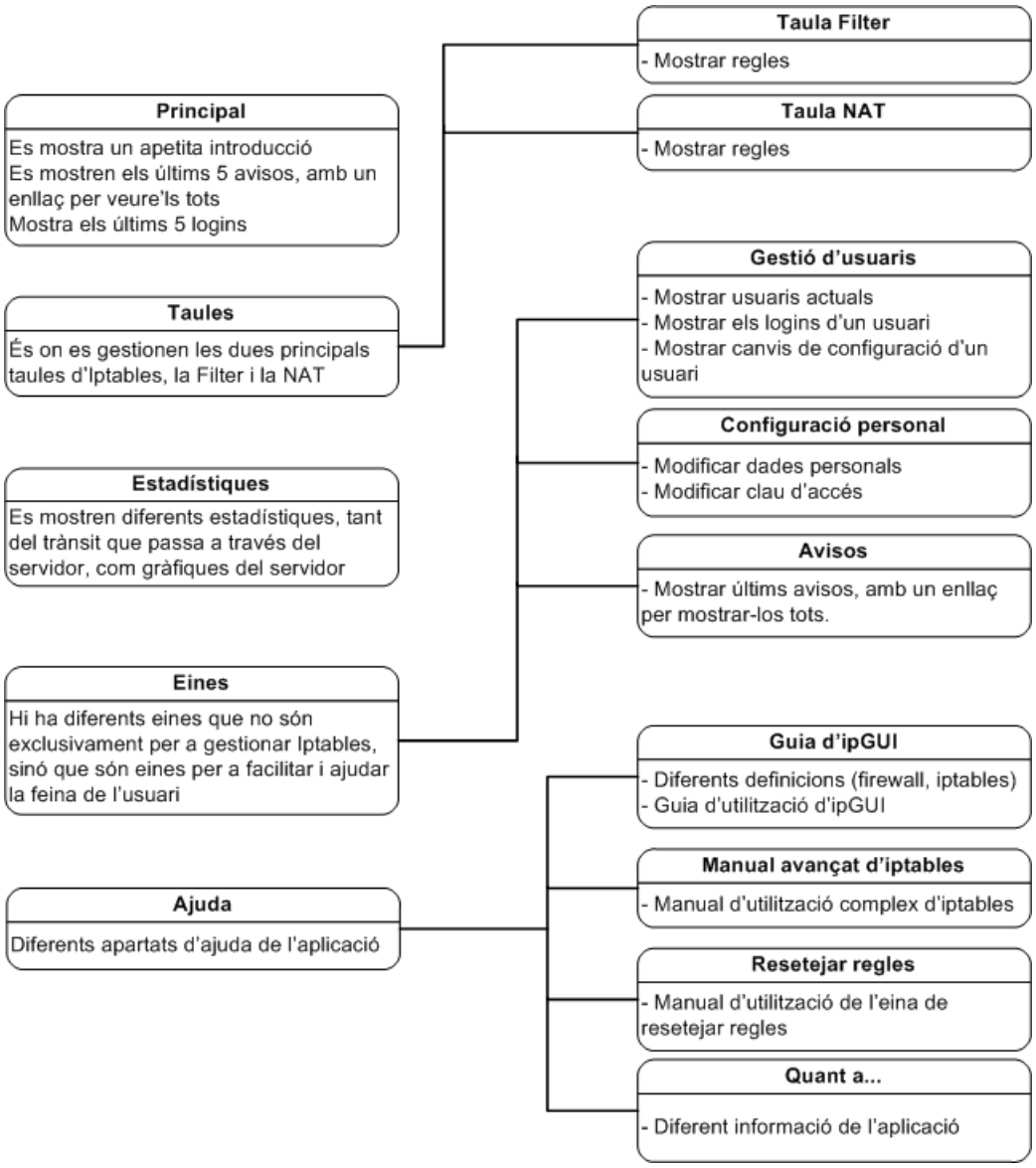

Figura 20: Mòduls per a un usuari invitat

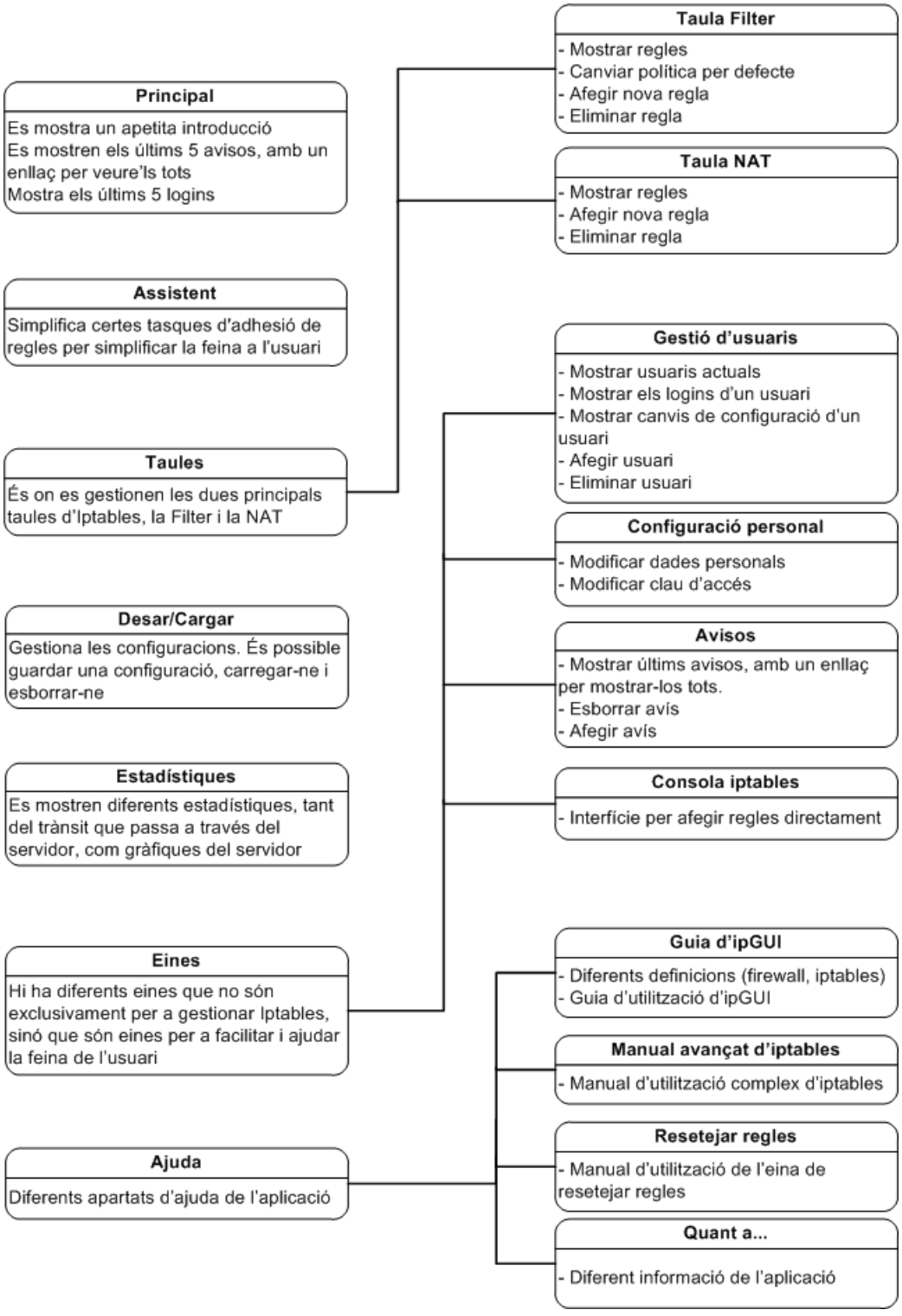

Figura 21: Mòduls per a un usuari administrador

Tots els arxius han d'estar degudament ordenats en carpetes, i creats amb noms curts però que n'identifiquin fàcilment la seva funció.

A l'inici de cada arxiu, hi ha d'haver una petita explicació del què fa, el codi ha d'estar comentat principalment en les parts on hi pot haver més confusió, com també correctament indentat i ordenat.

Tota l'aplicació ha de seguir un mateix ordre de disseny (colors, fonts, ordenació), utilitzant un mateix estil CSS[29]. Aquest disseny ha de ser senzill, clar, suau i agradable.

Quan s'hagin de mostrar llistats que poden ser llargs, l'aplicació els ha de poder paginar entre 30 i 50 entrades aproximadament. S'han de mostrar els botons per a poder navegar, però amagar'ls si no cal.

És important mostrar ajuda, sobretot en les parts on l'usuari ha de gestionar informació.

5.4 Navegabilitat

En aquest apartat es parlarà d'algunes eines que aporta l'aplicació per a facilitar la gestió a l'usuari. Es creu que és una part molt important ja que per a l'usuari final, ell l'únic que veu és aquesta part, com s'ha fet l'aplicació no li interessa massa, i per tant es farà una explicació bastant exhaustiva del què ofereix ipGUI.

Al loguejar-se, es redirigeix a la pàgina principal (figura 22), on es mostra una petita introducció, els últims avisos del sistema, i els últims logins d'usuari. Això permet que l'usuari vegi els avisos directament sempre que entra, ja que si hagués d'anar expressament a l'apartat d'avisos, segurament no ho faria, o no hi aniria sempre.

[29] http://en.wikipedia.org/wiki/Cascading_Style_Sheets

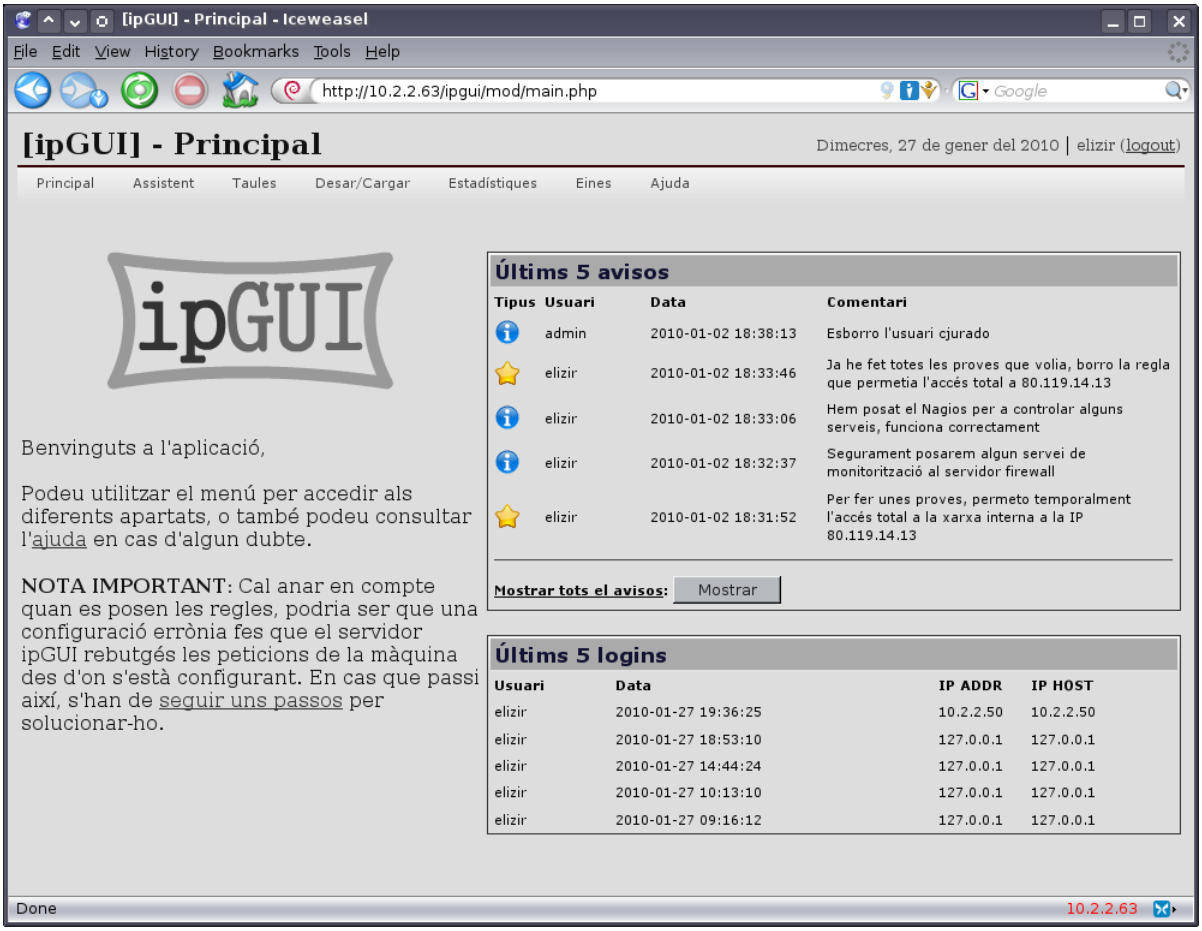

Figura 22: Pàgina principal

Ofereix menús, tant estàtics com dinàmics. Els estàtics serien aquells que fiqui on es fiqui l'aplicació, hi hauran sempre els mateixos components, com per exemple els protocols o les chains (que és difícil que n'hi hagi de noves).

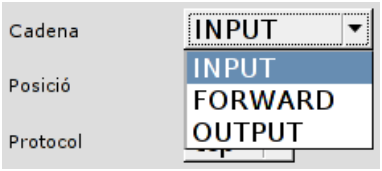

Figura 23: Menú estàtic: chains

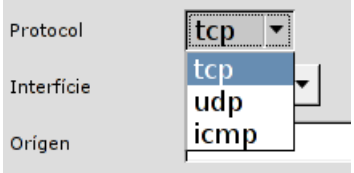

Figura 24: Menú estàtic: protocols

I el menús dinàmics, serien aquells en què poden variar en el sistema, o que es té previst que es puguin ampliar els components que el formen. Dels què poden variar en el sistema, l'aplicació n'ofereix tres, com són els de llistar les interfícies de xarxa del sistema (depèn el servidor en tindrà unes o altres), el llistat de configuracions que hi ha al sistema i que els usuaris han desat, o un llistat dels usuaris.

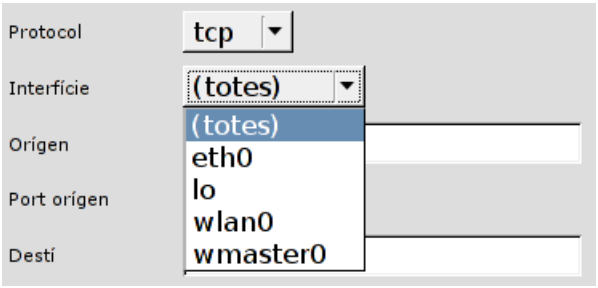

Figura 25: Menú dinàmic: interfícies

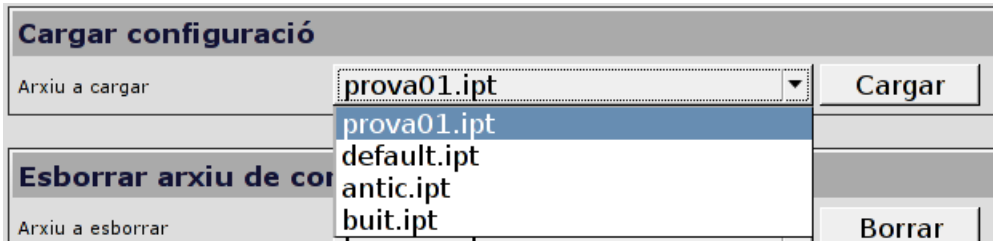

Figura 26: Menú dinàmic: arxius

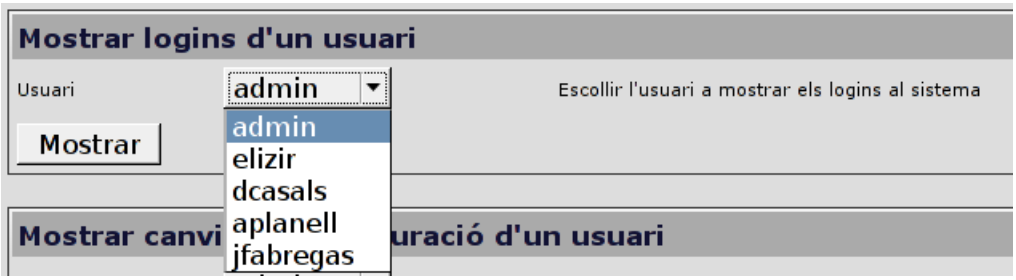

Figura 27: Menú dinàmic: usuaris

També hi ha un altre tipus de menú dinàmic, que no depèn del sistema directament, sinó que és ampliable per part de l'aplicació. Aquest és el de l'assistent d'obrir un servei, on hi ha un menú

desplegable on es mostren un seguit de serveis comuns, però que es pot ampliar en un arxiu de configuració. Per defecte, en l'arxiu "ipgui/config/conf.php":

```
// protocols permesos per l'assistent
$PROTOCOLS="http (80/tcp),80,tcp;https (443/tcp),443,tcp;ftp
(21/tcp),21,tcp;smtp (25/tcp),25,tcp;pop3 (110/tcp),110,tcp;telnet
(23/tcp),23,tcp;ssh (22/tcp),22,tcp;dns (53/udp),53,udp";
```

I en l'assistent es mostra:

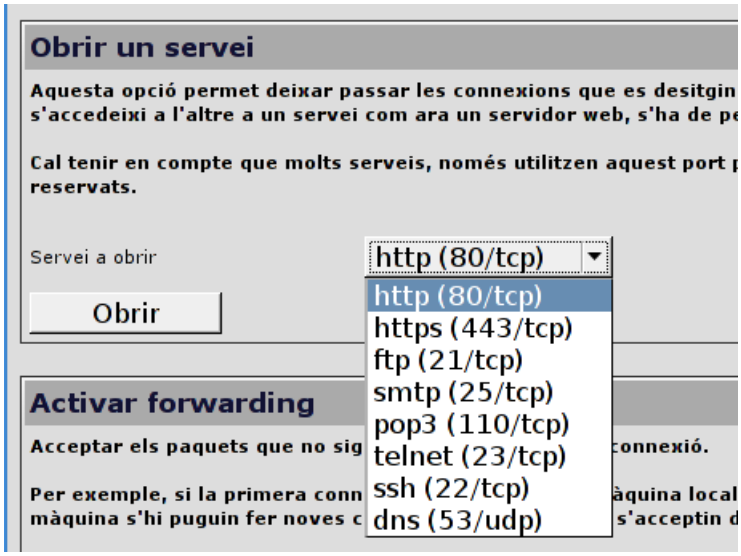

Figura 28: Menú dinàmic: serveis

Per tant, si es vol ampliar la llista, només cal modificar aquesta variable "$PROTOCOLS" i automàticament sortirà en el menú.

Un altre aspecte que s'ha aplicat per facilitar la feina de l'usuari, és el de modificació de les dades personals, on al entrar en aquell apartat, automàticament en el formulari es mostren les dades actuals.

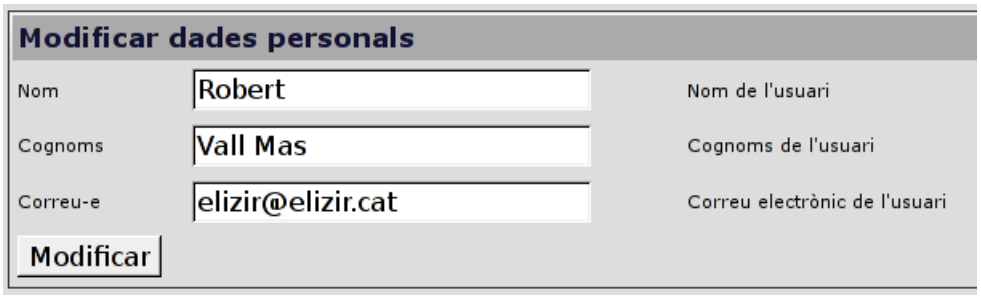

Figura 29: Formulari de modificació de les dades personals

En els formularis, s'han limitat els caràcters que hi ha en els llocs on l'usuari ha d'entrar dades manualment. Per exemple, al entrar el número de port, aquest està limitat a 5 caràcters ja que com a màxim serà el 65535, o un altre cas pot ser segons la limitació que existeix en la base de dades, de que si en un camp com podria ser el nom està limitat a 50 caràcters, l'usuari només en pot introduir 50. Això evita errors com ara que un usuari fiqui més del permès, i després quedi tallada la informació.

Als avisos també hi ha un parell de facilitats a l'usuari, com pot ser la d'introducció d'imatges per diferenciar els dos tipus d'avís, i el de mostrar el botó d'esborrar l'avís al costat de cada un (això en el cas dels administradors, si és un usuari invitat no se li mostra). També és important que els avisos estiguin ordenats i mostrats de més actuals a més antics, així sempre es mostren els més nous i importants en el moment de mostar-los.

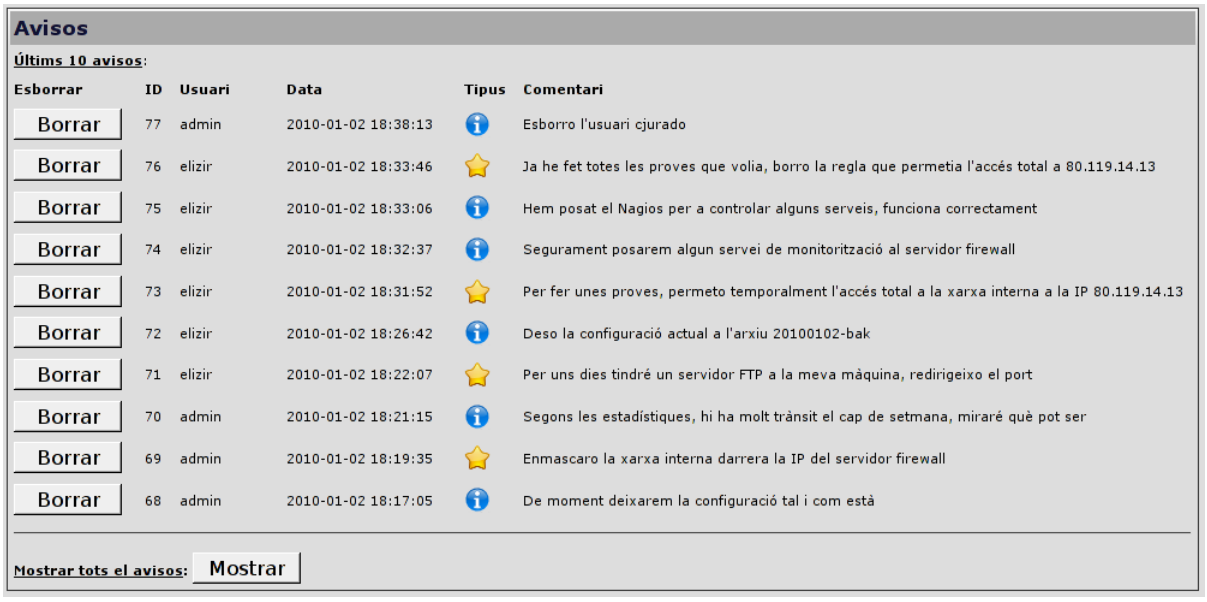

Figura 30: Llistat d'avisos (per un administrador)

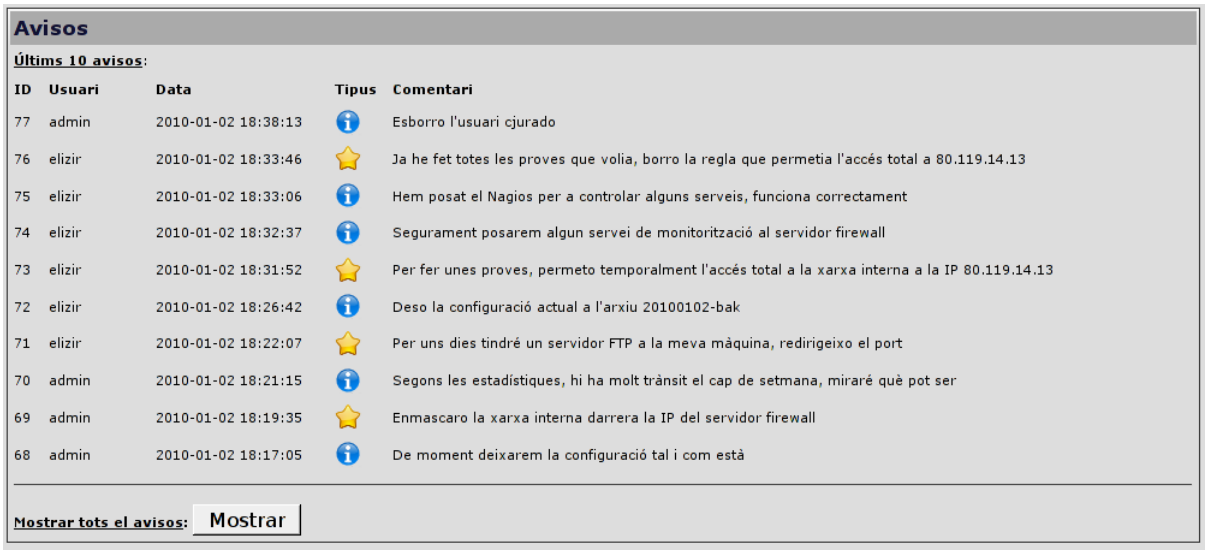

Figura 31: Llistat d'avisos (per un invitat)

Per a mostrar d'una forma més còmode llistats (logins d'usuari, logueig dels canvis al sistema dels usuaris, avisos) hi ha la paginació, que serveix per mostrar com a màxim 30 entrades, i amb la possibilitat de mostrar els el següents o anteriors. També és important que si en un llistat ja no queden més entrades, no es mostri el botó de posteriors entrades, la igual que amb el d'anteriors.

Figura 32: Botó de paginació

Figura 33: Botons de paginació

Un altre aspecte en la navegabilitat, és el de crear un índex amb enllaços en l'ajuda de la "Guia d'ipGUI", tal i com mostra la següent imatge.

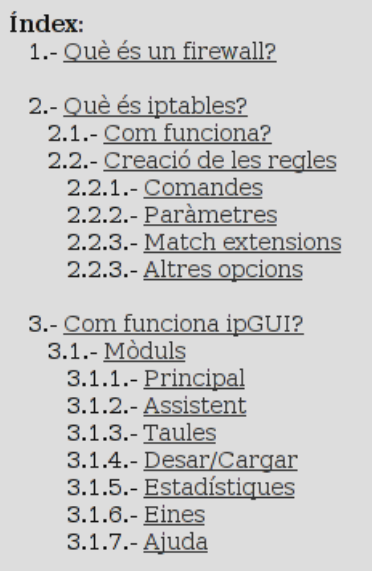

Figura 34: Índex d'ajuda

És molt important la comunicació amb l'usuari. Això significa que al fer alguna cosa, s'ha de confirmar aquestes accions mostrant la informació necessària. A continuació es mostren alguns exemples d'això.

- Bloquejar una màquina:

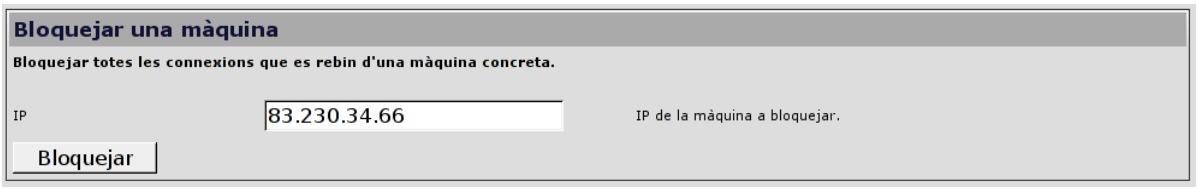

Figura 35: Assistent - Bloquejar màquina (abans)

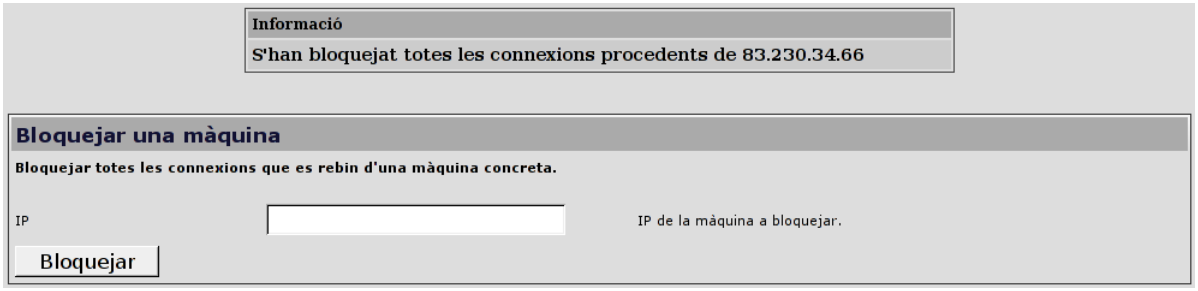

Figura 36: Assistent - Bloquejar màquina (després)

- Afegir avís:

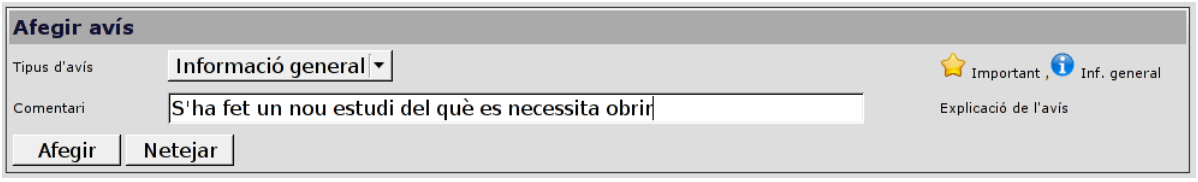

Figura 37: Afegir avís (abans)

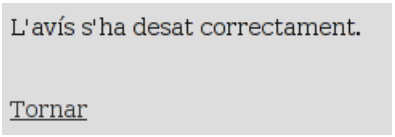

Figura 38: Afegir avís (després)

- Canviar el password de l'usuari (els passwords de confirmació no coincideixen):

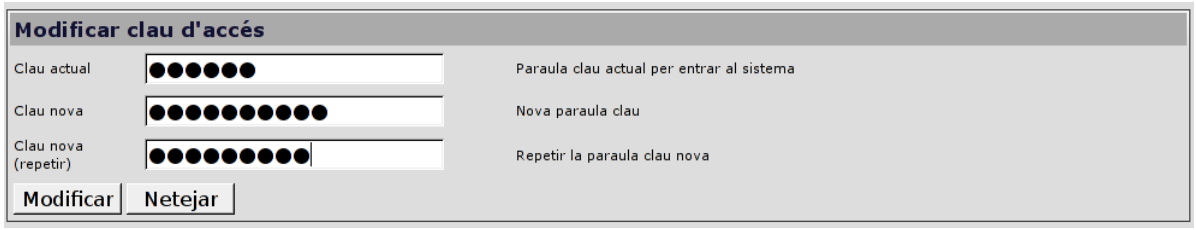

Figura 39: Modificació del password de l'usuari (abans)

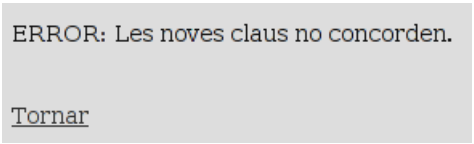

Figura 40: Modificació del password de l'usuari (després)

N'hi ha molts d'altres de missatges per l'usuari (cargar/guardar/esborrar fitxers de configuració, canviar dades d'usuari, noves regles creades/esborrades), i dels què fan referència a canvis en el *firewall*, són loguejats i guardats en nom de l'usuari que els ha fet.

En general, s'ha intentar fer més còmode la gestió a l'usuari, que indirectament incorpora el benefici que disminueix la possibilitat d'equivocar-se.

6 Implementació

Aquest apartat exposa com s'han acabat fent les coses, des de la instal·lació del software al servidor, les seves configuracions, els permisos dels fitxers, com estan organitzats els fitxers, etcètera.

És molt útil per fer-se una idea de com ha quedat finalment l'aplicació, i fins hi tot per tenir una guia per si mai es vol instal·lar ipGUI en algun servidor.

6.1 Instal·lació del servidor

Per a instal·lar Debian, s'ha fet una instal·lació bàsica del sistema operatiu (a partir d'un CD), s'han fet totes les actualitzacions de seguretat (via apt-get[30]), i llavors s'ha procedit a fer la resta d'instal·lacions.

Com ja s'ha comentat, iptables ja ve per defecte en els nuclis Linux. El què sí cal mirar és que en certes distribucions GNU/Linux, pot ser que no estigui activat, o que estigui activat però com a mòdul, en ambdós casos cal assegurar-se que s'activa al iniciar el sistema. En Debian, iptables ja bé compilat en el nucli, i per tant no cal activar'l ni res.

Com que una de les funcionalitats més comunes que se li pot donar a ipGUI és la d'utilitzar'l com a enrutador, s'ha habilitat al sistema per a què ho pugui fer sempre.

Per saber si un sistema GNU/Linux pot enrutar trànsit IP, només cal mirar el contingut de l'arxiu "/proc/sys/net/ipv4/ip_forward", si és un 0 és que no, i si és un 1 és que sí. Per a fer que enruti, hi ha diferents maneres, la més habitual és fer un script que s'executi a l'inici per a què fiqui un 1 en aquest arxiu, ja que al reiniciar aquesta variable pren el valor per defecte. En el projecte s'ha optat per canviar un paràmetre del kernel (nucli del sistema) de manera permanent, el què fa referència a l'anomenat *IP Forward*. Per fer-ho, s'ha editat el fitxer "/etc/sysctl.conf", canviant el paràmetre a:

```
net.ipv4.ip_forward = 1
```

Llavors per aplicar els canvis, només cal executar un parell de comandes:

[30] http://wiki.debian.org/Apt

```
root@projecte:~# sysctl -p /etc/sysctl.conf
net.ipv4.ip_forward = 1
root@projecte:~# /etc/init.d/procps restart
Setting kernel variables (/etc/sysctl.conf)...done.
```

I a partir d'ara, encara que es reinicii la màquina estarà activat.

La instal·lació del servidor web Apache2 s'ha fet via apt-get sense problemes. L'únic que s'ha hagut de fer per evitar que surti un missatge d'error, és afegir a l'arxiu /etc/apache2/httpd.conf la línia:

```
ServerName projecte
```

De la resta de configuració de l'Apache2, la què ve per defecte ja va bé. Cal tenir clar però quina és l'arrel des d'on llegeix l'Apache (on han d'anar els arxius de l'aplicació):

```
DocumentRoot /var/www/
```

Per instal·lar PHP, cal instal·lar el paquet en si, però també el mòdul per a l'Apache2, ja que sinó el servidor web no pot interpretar el llenguatge. Un cop tot instal·lat, per a activar el mòdul, s'ha d'executar la comanda "a2enmod", i escollir d'entre els mòduls disponibles per a l'Apache2 el de "php5".

En el cas de MySQL, és semblant al de PHP. S'ha d'instal·lar el servidor MySQL, i també el connector entre MySQL i PHP, en aquest cas el mòdul de MySQL per a PHP.

Per a què l'aplicació pugui accedir a la base de dades de MySQL, hi ha d'haver un usuari MySQL que pugui accedir a aquesta, i l'aplicació ha de conèixer aquest usuari, el password, el nom de la base de dades, i el lloc on està (habitualment a la mateix màquina). Aquestes dades han d'estar dins l'arxiu "/var/www/ipgui/config/conf.php", concretament en l'apartat:

```
/*
* configuracio connexio bbdd
*/
```

```
// nom de la base de dades

$MYSQL_BBDD = "ipgui";


// nom del host

$MYSQL_HOST = "localhost";


// nom de l'usuari de la bbdd

$MYSQL_USER = "ipgui";


// clau de l'usuari de la bbdd

$MYSQL_CLAU = "pfcipgui";
```

Llavors, ha de coincidir amb l'usuari que s'ha de crear a MySQL, on ha de tenir certs permisos sobre la base de dades d'ipGUI. Concretament: SELECT, INSERT, UPDATE, DELETE.

En l'apartat d'estadístiques, ja s'ha comentat que s'utilitza software extern instal·lat al servidor, i aquest és MRTG (figura 41) i Munin (figura 42). S'ha fet que les seves sortides estiguin accessibles per a l'Apache2, i així poder fer enllaços com a aquestes imatges. És a dir, si per exemple s'ha configurat que MRTG desi a "/var/www/mrtg/", des de l'aplicació s'accedeix a aquests resultats fent enllaços relatius de l'estil "../../mrtg/eth0-day.png".

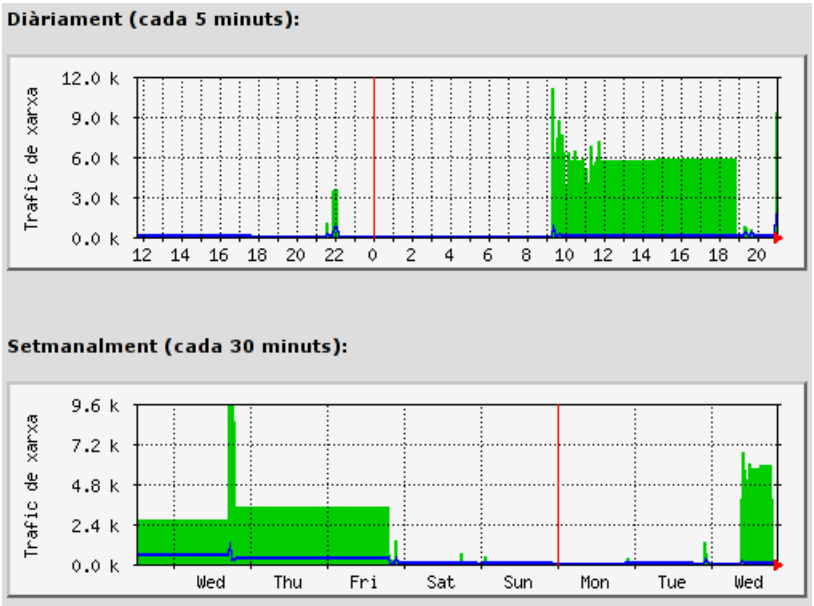

Figura 41: Algunes de les gràfiques de MRTG

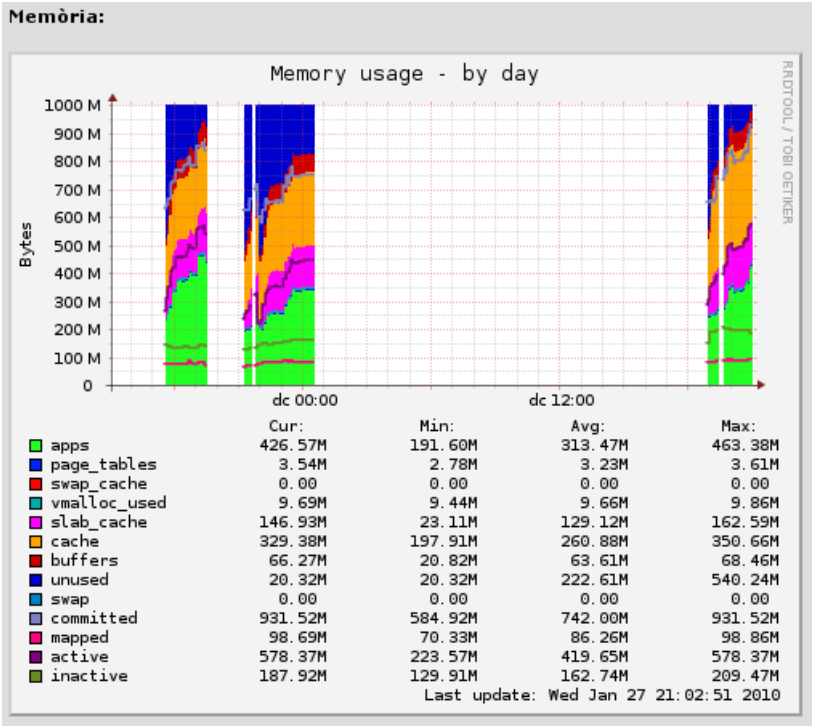

Figura 42: Algunes de les gràfiques de Munin

Per fer que l'Apache2 pugui accedir a una eina del sistema administrativa, ja s'ha comentat que s'ha utilitzat l'eina "sudo". Per a configurar'l, es fa a partir del seu arxiu de configuració "/etc/sudoers". En el cas d'aquesta aplicació, les línies de l'arxiu que s'han de canviar són:

```
# User alias specification

User_Alias DAEMONS = www-data , emergency


# Cmnd alias specification

Cmnd_Alias FIREWALL = /sbin/iptables, /sbin/iptables-restore,
/sbin/iptables-save


# User privilege specification

root ALL=(ALL) ALL

DAEMONS ALL = NOPASSWD: FIREWALL
```

Llavors, quan l'Apache vulgui utilitzar l'iptables, en la comanda només haurà de ficar "sudo" davant de tot, per exemple:

```
sudo /sbin/iptables -L -v -n
```

Bash no cal instal·lar-ho expressament, ja es fa per defecte al instal·lar Debian.

6.2 Distribució dels arxius de l'aplicació

S'ha intentat fer de la manera més clara possible, com per exemple separant tots els continguts segons la seva funció o ficar noms curts però clars.

El codi de l'aplicació està dins de la carpeta "/var/www/ipgui", però es fiqui on es fiqui funcionarà correctament perquè el codi està fet amb adreces relatives (sempre que l'Apache2 hi pugui accedir).

Els permisos que s'han donat per als arxius són els següents:

- Propietari de l'arxiu: Un usuari no administrador del sistema, i que hi pugui llegir i escriure.
- Grup de l'arxiu: El grup de l'Apache2 (www-data), pot llegir tots els arxius i carpetes, però no escriure-hi.
- Resta d'usuaris: Cap permís, ni llegir.

S'ha fet així pensat que era la millor manera i la més segura. Evitar que un usuari administrador en sigui el propietari, que l'Apache2 no pugui modificar res, i que la resta d'usuaris del sistema no puguin veure res.

Hi ha una excepció, i és la carpeta "/var/www/ipgui/saves". En aquesta carpeta és on es desen els arxius de configuració de l'iptables, que es gestionen a partir de l'aplicació. L'Apache2 ha de tenir permisos per escriure-hi, així que s'ha optat perquè el grup www-data hi pugui escriure:

```
drwxrwx--- 2 elizir www-data 72 16 gen 18:42 saves
```

Els arxius que es creïn aquí dins, com que els crea l'usuari del sistema de l'Apache2, els arxius seran propietat de www-data:

```
-rw-r----- 1 www-data www-data 396 17 nov 19:32 buit.ipt
```

L'aplicació està estructurada tal i com mostra la següent imatge:

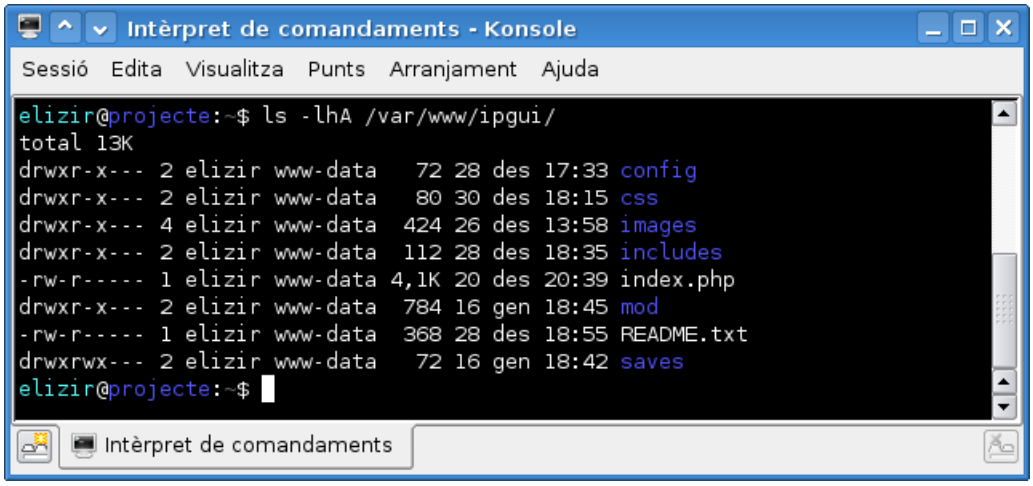

Figura 43: Arxius de la carpeta /var/www/ipgui

L'arxiu "/var/www/ipgui/index.php", és la pàgina de login. Si es logueja correctament, llavors es redirigeix a la pàgina principal (main.php), que està dins de la carpeta "mod". Dins d'aquesta carpeta, és on hi ha tots els mòduls de l'aplicació.

6.3 Distribució de l'aplicació

Un cop un usuari s'ha loguejat correctament, se'l redirigeix a la pàgina principal (mod/main.php), on se li mostra diferent informació com ara els últims avisos del sistema i els últims logins dels usuaris.

A partir d'aquí, i mitjançant el menú superior, es pot accedir a tots els mòduls de l'aplicació:

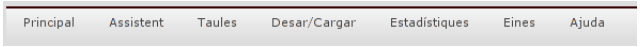

Figura 44: Menú principal

En algun d'aquests mòduls que mostra el menú hi pot haver sub-mòduls, com és el cas de "Taules", on hi ha els apartats "Taula Filter" i "Taula NAT".

En qualsevol moment, l'usuari pot anar lliurement d'un mòdul a un altre, ja que el menú superior es mostra sempre.

Quan l'usuari vulgui sortir, a dalt a la dreta de la pàgina hi ha el botó de desloguejar-se, on clicant es netejaran les variables de sessió i es redirigirà a la pàgina de login.

Si es vol conèixer una mica més sobre l'aplicació es pot consultar la guia d'utilització d'ipGUI, que està en els annexes a la pàgina 82.

6.4 Funcions

Totes les funcions estan dins dels arxius "includes/commands.php" i "includes/common.inc". El primer és on hi ha les funcions que fan referència principalment a les comandes per interactuar amb iptables, i el segon són principalment funcions per a insertar codi PHP.

De les funcions que hi ha dins de commands.php, per fer-se una idea a continuació es mostra la funció més simple que hi ha, la de borrar un arxiu de configuració:

```
// delarx - esborrar arxiu de configuracio
function delarx($arx, $DIR_SAV)
{
    echo exec("rm $DIR_SAV/$arx");
    // logejar comanda
    $cadena = "Ha esborrat l\'arxiu $arx";
    cmdlog($cadena);
}
```

La funció s'executa quan en el formulari de l'aplicació, es prem el botó de "Borrar". A la funció li arriba el nom de l'arxiu i el lloc on es troba, i després l'esborra. Dins la mateixa funció, se'n crida una altra (cmdlog) que és la de loguejar el què ha fet l'usuari (insereix informació a la base de dades).

S'ha intentat que aquestes funcions no fossin molt específiques per a fer una tasca concreta, que fossin polivalents. Per exemple, la funció per a crear una nova regla, serveix tant per la taula

Filter com per la NAT, i si alguns paràmetres no hi són no els té en compte i executa la comanda sense problema.

L'assistent que serveix per a crear regles, principalment s'aprofita d'aquestes funcions, ja que per a crear aquestes regles, es demana introduir algun valor important a l'usuari (com pot ser la direcció de la màquina implicada), i la resta de paràmetres s'introdueixen de manera automàtica segons la seva finalitat. Això simplifica molt la feina a l'usuari, sobretot si és inexpert.

De les funcions d'inserir codi PHP que és comú en les pàgines (com ara les capçaleres, menús, peus, ...), la més simple poder és la de tancar el codi HTML:

```
// final de la pagina (tancar tags body i html)
function pag_final()
{
    echo "\n\n<!------ /body ------>\n\n";
    echo "\n </body>\n";
    echo "</html>";
}
```

Això significa que en alguna pàgina, al cridar aquesta funció apareixerà aquest codi. Per cridar-la, és tant senzill com:

```
[...]
pag_final();
?>
```

Això és molt útil per vàries raons. Les principals:

- Estalvi de línies de codi repetides
- Sensible als canvis. Si mai es volgués canviar el codi per a totes les pàgines, si no es fes així s'hauria de canviar el codi de totes les pàgines. D'aquesta manera només cal canviar el codi de dins de la funció.

6.5 Ordenació del codi

Dins de cada arxiu de codi (principalment arxius amb l'extensió .php), hi ha una estructura determinada, des de la informació de què fa cada arxiu a l'inici o la comprovació de si l'usuari està loguejat, fins a com està ordenat el codi php.

Es creu que és molt important aquesta ordenació del codi (indentat) dins de la pàgina, així com ficar comentaris en els punts on és més complexe veure què fa. Un dels motius, és que resulta molt més fàcil trobar errors i canviar coses a posteriori. Un altre és que si aquesta aplicació l'ha de canviar algú que no ha participat en la seva creació, li resultarà molt més fàcil fer-ho, ja que identificarà molt més fàcilment les diferents parts.

```
81        echo "<br>\n";
82  }
83  unset($missatge);
84
85
86  // taula - regles actuals
87  echo "<center>\n";
88  echo "<table class=\"menu2\">\n";
89  echo " <tr class=titol><td colspan=2>Regles actuals</td></tr>\n";
90  echo " <tr class=peu>\n";
91  echo "  <td>\n";
92          showtable("filter", $SUDO_CMD);
93  echo "  </td>\n";
94  echo " </tr>\n";
95  echo "</table>\n";
96  echo "</center><br>\n";
97
98
99  // acces restringit, nomes administradors
100 if($_SESSION['tipus'] == "admin")
101 {
102       // taula - politica per defecte
103       echo "<center>\n";
104       echo "<table class=\"menu2\">\n";
105       echo "<form name=\"politiques\" method=\"POST\" action=\"./table-filter.php\">\n";
106       echo " <tr class=titol><td colspan=2>Política per defecte</td></tr>\n";
107       echo " <tr class=peu>\n";
108       echo " <tr class=peu>\n";
109       echo "  <td width=100>INPUT</td>\n";
110       echo "  <td>\n";
111       echo "   <select name=polinput>\n";
112       echo "    <option value=\"ACCEPT\">ACCEPT</option>\n";
113       echo "    <option value=\"DROP\">DROP</option>\n";
114       echo "   </select>  (Actualment: ";
115       // obtenir quina es l'actual politica per defecte
116       exec ("$SUDO_CMD/iptables -L -v -n |grep \"Chain INPUT\" |awk '{print $4}' ", $res);
117       echo "   $res[0])";
118       echo "  </td>\n";
```

Figura 45: Codi PHP indentat (Taula Filter)

També resulta important, que el codi HTML resultant del codi PHP surti ordenat. Sovint això no es té en compte, i al mirar el codi font d'algunes pàgines web resulta molt confús. En el codi de l'aplicació s'ha sigut molt estricte amb això, al igual que l'indentat del codi PHP.

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN" "http://www.w3.org/TR/REC-html40/loose.dtd">
<html lang="ca">
 <head>
  <meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
  <meta http-equiv="Content-language" content="ca" />
  <title>[ipGUI] - Principal</title>
  <link rel="stylesheet" type="text/css" href="../css/estil.css">
  <link rel="shortcut icon"  href="../images/favicon.ico">
  <script type="text/javascript">
  </script>
 </head>
 <body>
```

Figura 46: Codi HTML indentat

6.6 Eina de resetejar regles

Per a accedir a aquesta eina (evidentment cal fer-ho en local), cal loguejar-se amb l'usuari del sistema "emergency", llavors automàticament apareix el menú d'opcions. Al sortir d'aquesta, es deslogueja l'usuari.

Es vol que aquest usuari només pugui fer això, executar l'aplicació i prou, que no pugui accedir a l'intèrpret de comandes. Fins hi tot, en el cas que l'aplicació fallés o es cancel·lés (per exemple prement Ctrl+c), es desloguegi i no es pugui fer res més.

Per a fer això s'ha fet que la seva shell no sigui Bash ni cap altra, sinó que sigui directament l'aplicació. Això es pot fer a partir de l'arxiu "/etc/passwd", on en el cas d'aquest usuari:

emergency:x:1001:1001:Emergency,,,:/home/emergency:/home/emergency/tool.sh

On l'arxiu "/home/emergency/tool.sh" és l'script on surt el menú d'opcions. Per tant, quan l'usuari es logueji li apareixerà directament l'script i en cas de cancel·lar l'aplicació o sortir, es deslogueja.

El què fa l'script quan s'escull l'opció de resetejar les regles, és carregar a iptables la configuració d'un arxiu en què no hi ha regles, i les polítiques per defecte són les d'acceptar. Llavors sí que es pot accedir a l'aplicació remotament.

Cal tenir en compte que aquest usuari (emergency), també haurà de poder utilitzar les eines administratives, i per tant haurà d'estar configurat a "/etc/sudoers" igual que l'usuari de l'Apache2.

Només s'han de copiar els dos arxius dins de la carpeta de l'usuari i donar els permisos necessaris:

```
root@projecte:~# chown emergency: /home/emergency/*
root@projecte:~# chmod 400 /home/emergency/buit.ipt
root@projecte:~# chmod 500 /home/emergency/tool.sh
```

En els annexes a la pàgina 88 hi ha un manual d'utilització, i en l'apartat C.1 a la pàgina 90 hi ha el codi de l'script.

6.7 Carregar configuració al iniciar el sistema

Un dels objectius era el de que hi ha d'haver la possibilitat de carregar una configuració al iniciar el sistema. Si no hi ha això, cada cop que s'iniciés el servidor ipGUI, iptables no cargaria cap regla i manualment s'hauria de carregar la configuració des de l'aplicació, i això és inviable.

S'ha fet utilitzant un script que s'executa al inici, que el què fa és carregar la configuració de l'arxiu per defecte. L'script és "/etc/init.d/ipgui-load", està fet en Bash, i segueix l'estructura que ha de tenir un script que s'executa al iniciar el sistema.

Per ficar'l en un sistema, simplement s'ha de copiar aquest script dins de la carpeta /etc/init.d/, donar permisos d'execució:

```
root@projecte:~# chmod 750 /etc/init.d/ipgui-load
```

I executar:

```
root@projecte:~# update-rc.d ipgui-load defaults
 Adding system startup for /etc/init.d/ipgui-load ...
   /etc/rc0.d/K20ipgui-load -> ../init.d/ipgui-load
   /etc/rc1.d/K20ipgui-load -> ../init.d/ipgui-load
   /etc/rc6.d/K20ipgui-load -> ../init.d/ipgui-load
   /etc/rc2.d/S20ipgui-load -> ../init.d/ipgui-load
   /etc/rc3.d/S20ipgui-load -> ../init.d/ipgui-load
   /etc/rc4.d/S20ipgui-load -> ../init.d/ipgui-load
   /etc/rc5.d/S20ipgui-load -> ../init.d/ipgui-load
```

Això el què fa és ficar els diferent enllaços corresponents a les carpetes adequades (les de l'init, que són les de l'arranc del sistema). Si es desitja, es pot utilitzar l'aplicació "rcconf" que ofereix Debian, on surt un menú amb tots els scripts de la carpeta i només s'ha de marcar si es vol que s'executi o no al iniciar.

En principi no cal modificar l'script, però cal repassar si la ruta de l'arxiu a carregar és correcte (variable $FILE).

En els annexes, en l'apartat C.2 a la pàgina 92 hi ha el codi de l'script.

7 Proves i problemes sorgits

A continuació es comentaran els principals problemes sorgits durant el projecte, i també es comentaran i mostraran algunes de les proves principals de funcionament que s'han fet al finalitzar la codificació.

7.1 Principals problemes trobats

En l'etapa de codificació, ja es feien les proves per a fer que el mòdul/funció en qüestió que s'estava codificant estigués el més depurat possible i no dongués errors. Així, al tenir gairebé finalitzat el projecte i al fer les proves finals, s'han detectat pocs problemes, i han sigut coses de poca importància com ara faltes d'ortografia o alineacions dels objectes a la pantalla.

Els principals problemes han sigut:

- El principal, poder saber comprendre el funcionament d'iptables, per a després poder fer una interfície amigable, saber l'estructura que ha de tenir una regla, i el seu funcionament en general.

  Realment no és molt amigable la seva configuració i interpretació, però per altra banda és molt potent i configurable, el qual el fa molt difícil de poder gestionar gràficament.

- La codificació de la llengua. No es sabia exactament com mostrar per pantalla text amb accents o paraules amb "ç" per exemple. Al principi es va pensar de en casos com ara per paraules amb"í", al codi ficar el seu equivalent "í", però després es va trobar una manera molt millor i més ràpida, que és d'afegir a la capçalera de la pàgina:

  ```
  <meta http-equiv="Content-Type" content="text/html; charset=UTF-8">
  <meta http-equiv="Content-language" content="ca">
  ```

- Accés a la base de dades mitjançant el connector MySQLi. És una mica diferent de l'habitual MySQL, i al principi costava una mica ja que molts cops no es ficava alguna cosa essencial que no es fica de la manera habitual, i després no funcionava bé.

- Els habituals problemes en la programació en PHP i MySQL, i en trobar maneres de com saber perquè una cosa no funciona.

7.2 Espai de treball utilitzat

Per a desenvolupar el projecte s'ha utilitzat un netbook, concretament un Toshiba NB200-10Z. Aquest té dues interfícies físiques de xarxa, una ethernet i una wifi. Les proves s'han realitzat connectant un switch a la targeta ethernet del servidor ipGUI, les màquines clients connectades a aquest mateix switch i tenint com a porta d'enllaç ipGUI, i fent que la sortida a Internet es fes a partir de la targeta wifi del servidor ipGUI:

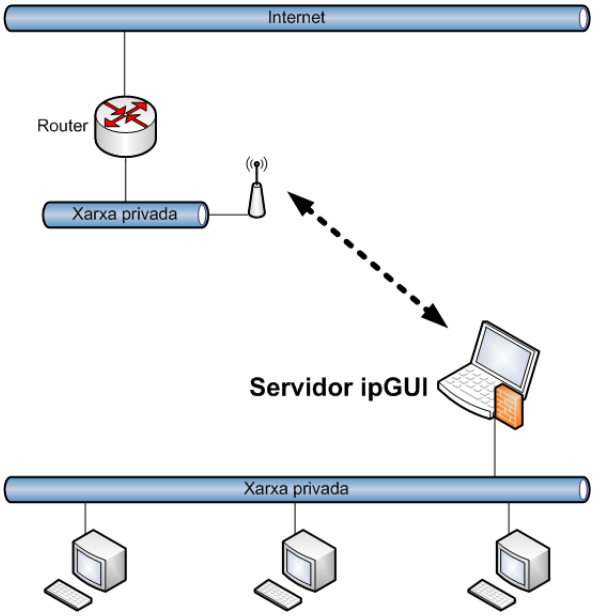

Figura 47: Esquema 1 de la xarxa de proves

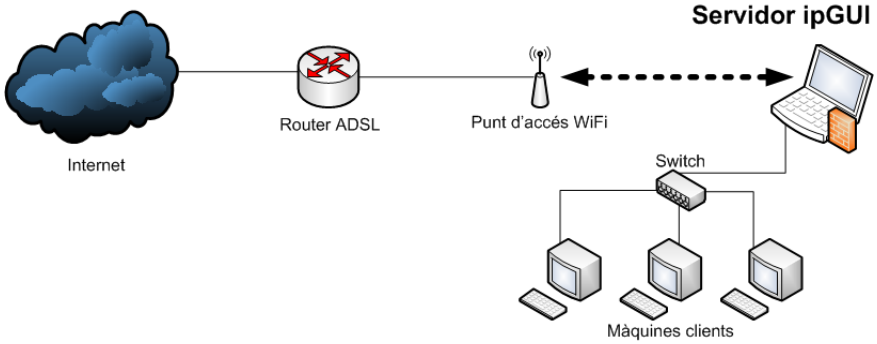

Figura 48: Esquema 2 de la xarxa de proves

7.3 Proves

L'aplicació està optimitzada per a una resolució de 1024x768, però s'ha provat amb resolucions de fins a 1680x1050 correctament.

S'ha comprovat el correcte funcionament sota els següents navegadors:

- Firefox 3.x - www.mozilla.com/firefox
- Internet Explorer 7.x i 8.x - http://www.microsoft.com/windows/Internet-explorer
- Konqueror 3.x i 4.x - www.konqueror.org
- Opera 10.x - www.opera.com
- Google Chrome 3.x - www.google.com/chrome
- Safari 4.x - www.apple.com/safari

Per a provar com és d'intuïtiva l'aplicació, es va deixar provar a un usuari sense molts coneixements informàtics. Se li va demanar que després de loguejar-se, accedís a certs llocs de l'aplicació, com ara que canviés el nom d'usuari o que consultés l'ajuda, i ràpidament hi va anar.

Després donant-li certes dades com ara unes IP's i ports, se li va demanar que afegís una regla, i seguint l'aplicació ho va poder fer.

Això demostra que ipGUI no requereix de grans coneixements tècnics, l'aplicació en si és intuïtiva, i si es volen fer coses més complicades, amb l'ajuda que ofereix el sistema no resulta molt complicat.

A continuació, es mostrarà una de les moltes proves finals, veient-se amb captures de pantalla. Això pot servir per fer-se una idea més clara de com funciona ipGUI. Aquesta prova consisteix en afegir una nova regla i després esborrar-la:

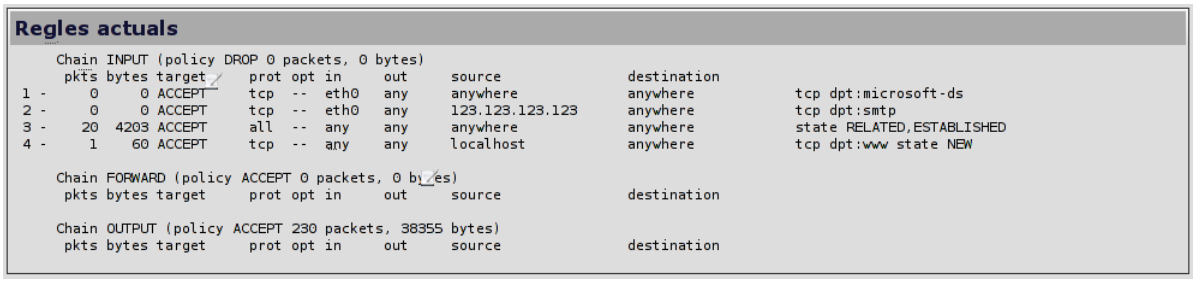

Figura 49: Estat de les regles abans d'afegir-ne una

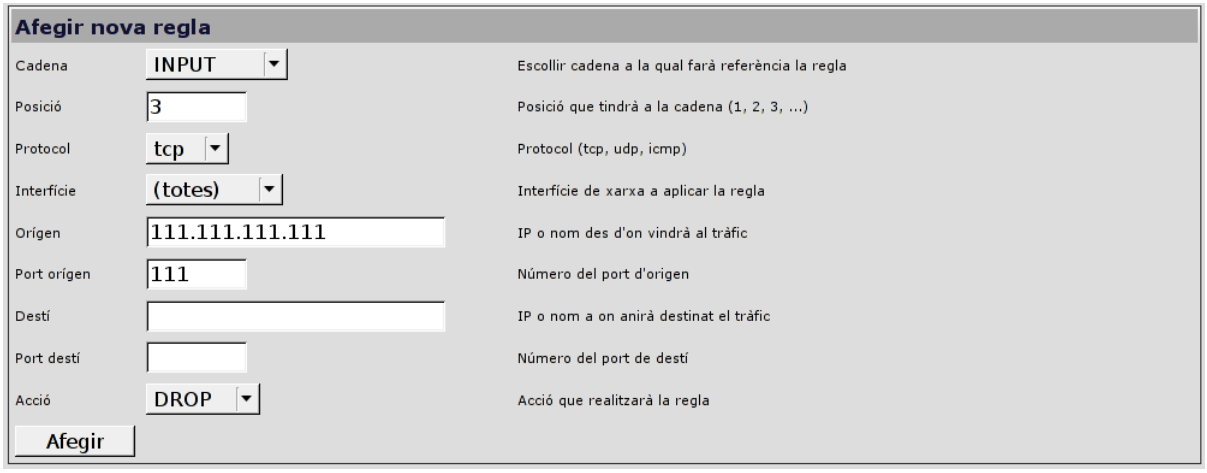

Figura 50: Formulari d'afegir nova regla

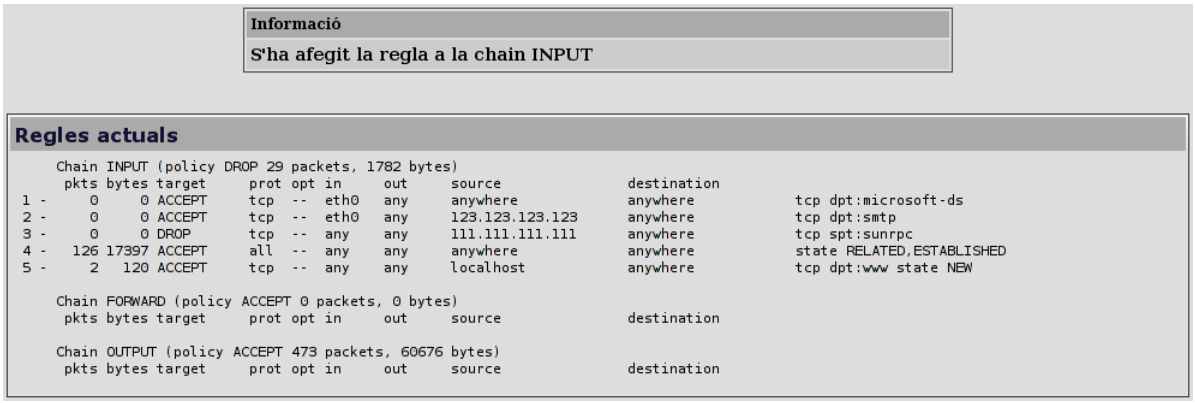

Figura 51: Estat de les regles després d'afegir-ne una

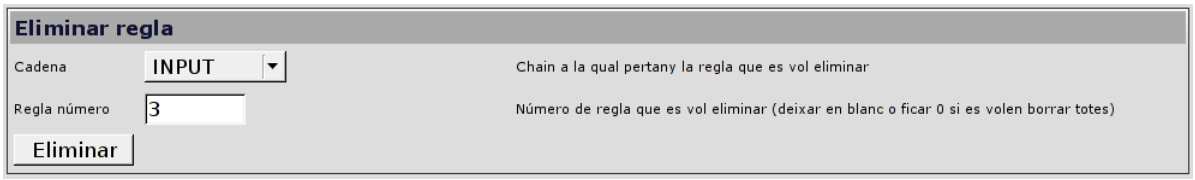

Figura 52: Formulari d'esborrar regla

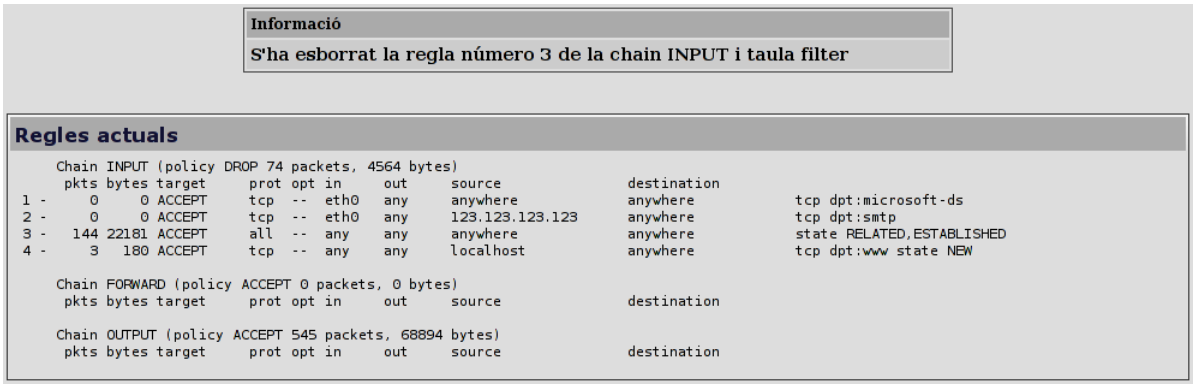

Figura 53: Estat de les regles després de borrar-ne una

8 Conclusions i futures línies de treball

8.1 Conclusions finals

Un cop finalitzada la codificació i gairebé acabada la memòria del projecte, és moment de fer una mirada enrere per veure la cronologia que ha sigut tot el procés. Des dels inicis on es pensava si fer realment un projecte com aquest, pensar com havia de ser l'aplicació, la fase de codificació, etcètera. I pot resultar curiós com ha anat tot mentre s'escriuen aquestes conclusions finals.

Aquest projecte, ha intentat centrar-se en el seu objectiu principal, i posteriorment en els secundaris. Una de les coses més importants (o la principal), és que s'han assolit tots aquests objectius plantejats inicialment, i fins hi tot se'n han aconseguit d'altres que es van afegir posteriorment.

Entre les virtuts que es considera que ha adquirit ipGUI, es pot destacar principalment la facilitat d'ús, molt difícil al intentar configurar una eina tant complexa com és iptables. Per a completar-ho, s'han afegit tot un seguit d'eines que es pensa que realment poden ser de molt ajuda als usuaris, cosa que molt poques eines que ja existeixen ho tenen. En general, una eina força completa, i el més important, realista dins el context actual.

Durant tot el procés s'han adquirit molt coneixements, des de programació en PHP i Bash, comunicació amb MySQL, en sistemes GNU/Linux, xarxes, i d'altres. El fet de no haver utilitzat cap eina de desenvolupament web (com podria ser Dreamweaver o NetBeans), ha servir per aprendre PHP encara en més profunditat. Per a fer el codi s'ha utilitzat el Vim[31], que és un editor de text en mode consola, i que pot resultar molt engorrosa la seva utilització, però que quan es fa servir un temps resulta molt potent, i es creu interessant també comentar això perquè, com s'ha comentat, són molts els coneixements adquirits de manera directa com indirecta.

Es creu que pel temps que s'ha tingut per fer el projecte, els resultats obtinguts són molt bons. Evidentment, tot és millorable, però l'autor material del projecte, ha acabat força orgullós del treball fet, dels coneixements adquirits i del resultat. L'experiència en general, ha sigut molt positiva.

[31] http://www.vim.org/

8.2 Futures millores

En general l'aplicació compleix bastant bé la seva feina, gestionar iptables, i a part d'això ofereix bastantes eines més que fan que l'aplicació sigui força més completa. Tot i això, si en un futur es vol millorar i ampliar-la, hi ha certes coses que es creuen que serien interessants, que són les què s'explicaràn a continuació.

Pel què fa a la gestió i configuració d'iptables, actualment hi ha la possibilitat d'una alta complexitat en la creació de regles, però no tot el ventall de possibilitats que ofereix iptables. Si bé és veritat que per a casos en què l'aplicació no dongui la possibilitat de fer alguna cosa que iptables sí permet, ipGUI té l'eina "Consola d'iptables" que és per interactuar-hi directament, seria millor aportar un grau més alt de complexitat i possibilitats en els mòduls de les taules Filter i NAT. Per a fer això últim, i tenint en compte la gran complexitat d'iptables, podria resultar molt complicat, ja que hi ha opcions que depenen d'altres que estan a la mateixa regla, i amb un formulari HTML estàtic no es pot fer bé. Per a fer-ho, segurament el més adient seria utilitzar AJAX[32], fins hi tot sense haver d'utilitzar XML[33], només amb JavaScript asíncron barrejat amb PHP.

Una altra possible millora que s'ha fet en part però no totalment, és la de control intern de l'aplicació. És a dir, per exemple quan es crea un usuari, demana el nom, cognoms, correu electrònic, etcètera, doncs al afegir un usuari es controla si hi ha un nom d'usuari igual (i en aquest cas avisa d'això i no afegeix l'usuari), però no de que el correu electrònic sigui correcte (que tingui un @, que no hi hagi espais, ...). No és una cosa que sigui molt complicada, i per a les coses més importants ja s'ha aportat aquest control, però s'ha pensat que valia més la pena passar-se més hores en fer altres funcionalitats més importants per a l'aplicació que no pas això. Per tant, en futures versions seria interessant aportar un millor control d'això.

Per últim, es creu que seria interessant utilitzar una connexió segura entre el servidor i el client, és a dir, https[34] en comptes de http[35].

[32] http://en.wikipedia.org/wiki/Ajax_(programming)
[33] http://en.wikipedia.org/wiki/XML
[34] http://ca.wikipedia.org/wiki/HTTPS
[35] http://ca.wikipedia.org/wiki/HTTP

8.3 Desviacions en la planificació

Respecte a la planificació de l'estudi de viabilitat que està a la pàgina 20, hi han hagut alguns canvis respecte a com s'ha portat en la realitat.

Es tenia previst que el projecte durés unes 236 hores. En algunes tasques, s'ha retallat el temps previst, i en d'altres s'ha allargat, però es calcula que en total les hores destinades a fer el projecte han estat unes 270 hores.

La diferència més important ha sigut en la planificació per part de la documentació. S'havia previst destinar unes 20 hores, i realment han sigut forces més, gairebé el triple. Les captures de pantalla, no saber exactament com ficar les coses i ordenar-les, omplir continguts, buscar informació addicional, etc... Ho han allargat molt més del previst.

En la part de la codificació sorprenentment es calcula que s'han complert les hores previstes aproximadament. En el temps destinat a aquesta tasca, també s'ha aprofitat per fer proves exhaustives, fent que les hores destinades a fer les proves finals hagin sigut menys.

Una altra de les parts de la planificació que s'han desviat una mica de la prevista ha estat la del temps destinat a l'Estudi de característiques del servidor, que estaven planejades uns 30 hores, però finalment es va estar buscant informació i decidir durant aproximadament unes 20 hores.

Per tant, es creu que fer unes 34 hores més del previst és dolent, però que no s'ha fet d'una manera exagerada i que és raonable. Més, pensant que s'han aportat algunes funcionalitats extres a l'aplicació, que s'han aplicat posteriorment de fer el disseny, donant prioritat en fer l'eina més completa (com són les estadístiques, els avisos, i altres) i no en complir escrupolosament el plaç.

El projecte es va iniciar entre finals d'octubre i principis de novembre del 2009, amb la intenció d'entrega'l per a la convocatòria de febrer. Poder era poc temps, però l'autor disposava de temps suficient totes les tardes i els caps de setmana. A principis de gener de 2010 la codificació estava pràcticament enllestida totalment a falta de quatre retocs, i dins el mateix mes es va fer la memòria.

De les 270 que es calcula aproximadament que va durar el projecte, exceptuant alguns dies en què no s'ha fet res, durant els 3 mesos que ha durat el projecte toquen unes 4 hores al dia de feina. Hi ha dies (i nits) que s'hi ha dedicat més temps, i d'altres que en estones lliures. Val a dir que les primeres setmanes van ser molt productives i que es va avançar molt, i en les últimes

el temps dedicat va ser més a polir algunes coses que en avançar.

A continuació, es mostrarà una compartició entre la planificació prevista inicialment en el projecte, i la real, la què s'ha acabat produint.

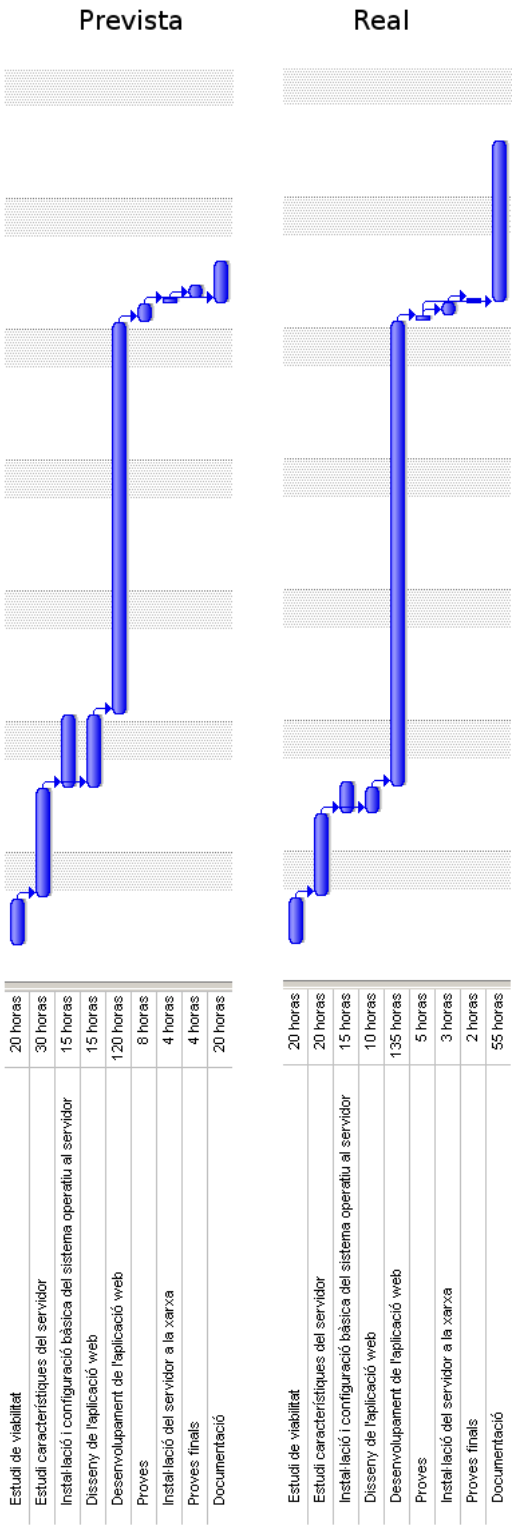

Figura 54: Comparació de la planificació

9 Bibliografia

La gran majoria d'informació que s'ha necessitat per a fer aquest projecte, s'ha extret d'Internet. De llibres pràcticament no se'n ha utilitzat cap, els pocs que es van consultar, o estaven desfasats o es van trobar coses millors.

A continuació es mostraran les fonts d'informació més utilitzades.

Documentació iptables:

- http://www.netfilter.org/documentation/
- http://www.pello.info/filez/firewall/iptables.html
- http://catux.org/articles-mainmenu-38/20-servidor/188-com-usar-el-millor-firewall-de-gnulinux-netfilteriptables-1

Documentació PHP:

- http://php.net/docs.php
- http://www.phpclasses.org
- http://w3schools.com/php/

Guies per fer la memòria:

- Projecte de final de carrera "Interfície Web Firewall Linux", UAB Sabadell, any 2008.
- Projecte de final de carrera "Aplicación de gestión integral para administraciones de lotería", UPM, any 2009, http://oa.upm.es/1829/ .

Altres:

- Activar *IP Forward* sota Linux: http://www.ducea.com/2006/08/01/how-to-enable-ip-forwarding-in-linux/
- Casos d'ús: http://www.cvc.uab.es/shared/teach/a20363/uml1.pdf

Annexes

A Guia d'ipGUI

Aquí es mostrarà una guia bàsica d'utilització de l'aplicació ipGUI, per començar a aprendre el seu funcionament i característiques.

A.1 Com funciona ipGUI?

Com ja s'ha dit, el què fa ipGUI és gestionar l'iptables, i es fa a partir d'una interfície web.

Ofereix una àmplia configuració d'iptables a partir de formularis, fent molt més fàcil la seva gestió. També ofereix altres funcionalitats extra, com poden ser:

- Estadístiques.
- Gestió d'usuaris, com ara afegir usuaris, mostrar quan s'han connectat al sistema, els canvis que han aplicat al *firewall*, ...
- Avisos.
- Possibilitat de fer canvis als propis perfils dels usuaris.
- Diferents tipus d'ajuda i guies.
- Eina per a la restauració del sistema en cas de fallada.
- I altres.

Per a loguejar-se, només cal un navegador. Cal però que s'hi tingui accés en xarxa i que no hi hagi regles que impedeixin connectar-s'hi. A la barra de navegació, cal ficar la IP o el nom de la màquina, i a continuació "/ipgui". Per exemple, si la IP és 10.1.1.2, s'ha de ficar "http://10.1.1.2/ipgui":

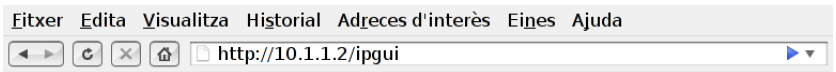

Figura 55: Barra de navegació d'un navegador web

Llavors sortirà una pàgina on s'ha de ficar el nom d'usuari i el password:

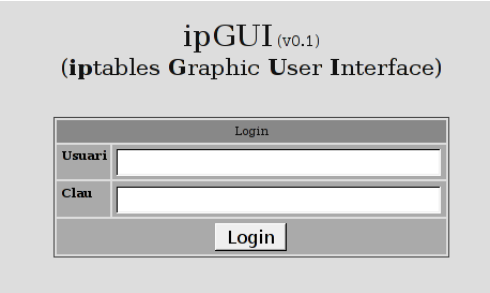

Figura 56: Autenticació

Cal tenir en compte el tipus d'usuari amb què s'hagi loguejat. N'hi ha de dos tipus:

- **Administrador**: Poden fer ús de totes les opcions de l'aplicació sense restriccions.
- **Visualitzador**: Tenen accés solament a aquells apartats on només es mostra informació, però no poden fer cap canvi al sistema. L'únic canvi que poden fer és referent al seu compte personal, com ara canviar el correu electrònic de contacte i altres.

Un cop s'està loguejat, només cal anar als mòduls que es desitgin a partir del menú principal que està a dalt de la pàgina:

Figura 57: Menú principal

A continuació, una descripció dels diferents mòduls (cal tenir en compte que si un usuari no és administrador, alguns dels apartats que s'explicaràn no se li mostraran).

A.1.1 Principal

Pàgina principal, que és la què es mostra al loguejar-se.

Aquí es pot observar els últims 5 avisos del sistema, i els 5 últims accessos a l'aplicació dels usuaris.

A.1.2 Assistent

Són diferents assistents per a poder desenvolupar certes accions concretes (creació de regles), que són usuals i útils, fent que sigui molt fàcil la seva aplicació.

En cada apartat ja està descrit per a què serveix, i també tots els camps que s'han d'omplir.

A.1.3 Taules

Figura 58: Menú principal - Taules

Com s'ha descrit anteriorment, les dues taules principals són la Filter i NAT. Des d'aquí es pot accedir a aquestes dues taules:

- Taula Filter
- Taula NAT

La configuració de les dues taules és similar. En l'apartat "Regles actuals", mostra les regles de cada taula, amb el número de regla al principi.

A "Política per defecte", que només és operatiu per a la taula Filter (a NAT està obsolet), es pot escollir quina es vol per a cada chain.

Per a afegir una nova regla, hi ha l'apartat "Afegir nova regla", on ja es descriu cada camp. Si en algun camp no s'hi escull res, s'aplicarà l'opció per defecte. Per exemple, si no s'especifica cap port d'origen, en aplicar la regla per defecte s'aplicarà per a tots els ports.

Si es vol eliminar una regla concreta, en l'apartat "Eliminar regla", s'escull la chain a la què pertany la regla, com també el número de regla que es pot veure en l'apartat "Regles actuals".

A.1.4 Desar/Cargar

La configuració de l'iptables pot ser desada i cargada a partir de fitxers. En aquest apartat es poden gestionar aquests arxius.

Es pot desar la configuració actual en un arxiu en l'apartat "Desar configuració actual". En un desplegable que mostra tots els arxius de configuració que hi ha, dins de "Cargar configuració", on es carrega la configuració de l'arxiu i sobreescriu l'actual. I en l'apartat "Esborrar arxiu de configuració", que també hi ha un desplegable amb els arxius que hi ha, es pot escollir l'arxiu a borrar.

Si es vol que una configuració es carregui al iniciar-se el servidor, s'ha de desar la configuració amb el nom de "default".

A.1.5 Estadístiques

En aquest apartat es mostren diferents estadístiques del sistema, principalment del tràfic de les interfícies de xarxa, i també altres que poden ser interessants referents a l'estat del servidor.

A.1.6 Eines

Figura 59: Menú principal - Eines

Aquí hi ha diferents apartats que fan referència a la gestió de diferents funcionalitats, però que no són per a la configuració del *firewall* (excepte una), com poden ser gestió d'usuaris i altres aspectes. Aquests apartats són:

- Gestió d'usuaris
- Configuració personal

- Avisos
- Consola iptables

A "Gestió d'usuaris" es mostren els usuaris actuals del sistema, es mostren els logins que ha fet un usuari en concret (quan s'ha loguejat a l'aplicació), es mostren els canvis que ha fet un usuari en la configuració del *firewall*, i es poden afegir i esborrar usuaris.

Dins "Configuració personal" es poden modificar les dades de l'usuari (només les seves), com també el password.

En el mòdul d'"Avisos", es gestionen els avisos del sistema. Aquests avisos s'utilitzen principalment per a informar als altres usuaris de canvis al sistema o altres informacions.

Aquests avisos poden ser etiquetats segons siguin importants (⭐) o siguin d'informació general (ℹ), i també poden ser borrats de manera individual.

Si l'aplicació ipGUI, no ofereix la possibilitat de realitzar alguna acció concreta de l'iptables, en la "Consola iptables" hi ha la possibilitat d'executar directament comandes d'iptables utilitzant l'intèrpret de comandes.

Per a realitzar algunes accions complexes, s'ha de tenir un nivell alt de coneixement de l'iptables, i per això es disposa d'un manual avançat d'iptables (en anglès).

A.1.7 Ajuda

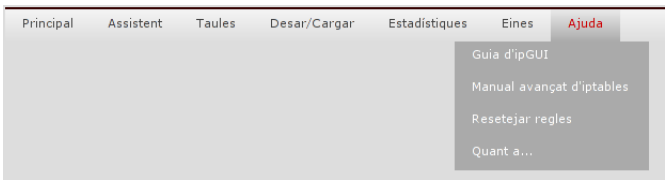

Figura 60: Menú principal - Ajuda

Aquí es disposa de diferents manuals d'ajuda i d'informació. Aquests apartats són:

- Guia d'ipGUI
- Manual avançat d'iptables

- Resetejar regles
- Quant a...

En la "Guia d'ipGUI" s'explica què és un *firewall*, què és iptables, i també hi ha un manual d'ús de l'ipGUI.

Dins el "Manual avançat d'iptables" hi ha un manual molt complet d'iptables, per si es necessiten realitzar regles més complexes.

En l'apartat "Resetejar regles" hi ha un manual que indica els passos que s'han de seguir en el cas de que s'hagi configurat el *firewall* de tal manera, que no es pugui accedir a l'aplicació, i per tant s'han de borrar totes les regles existents.

I el l'últim apartat "Quant a...", hi ha una breu informació sobre l'aplicació ipGUI.

B Resetejar regles

L'administració d'aquesta aplicació, sovint es farà remotament. Pot passar que al aplicar algun canvi a la configuració del *firewall*, el servidor denegui per exemple tot el tràfic cap al seu port 80 (servidor web, per on s'accedeix a l'aplicació), i no es puguin fer canvis ja que denega les peticions.

Per a casos com aquest, s'ha habilitat una eina per a poder resetejar les regles, i per tant poder tornar a accedir a l'aplicació.

En el pitjor dels casos, el servidor *firewall* denegarà tot el tràfic cap a ell, per tant, l'eina s'ha d'executar en local (directament al servidor). Consisteix simplement en loguejar-se com a usuari "emergency", i automàticament s'obrirà una aplicació en que demanarà què fer de manera senzilla utilitzant un menú. Això el què farà, serà netejar totes les regles de l'iptables, permetent després poder accedir a l'aplicació altre cop.

Instruccions:

1. Obrir un terminal, i loguejar-se com a usuari "emergency". La clau per defecte és "emergency", però podria ser que en la instal·lació s'hagués canviat. En aquest cas, cal contactar amb l'administrador del servidor.

2. Un com s'hagi loguejat correctament, automàticament sortirà l'aplicació.
   Només cal seguir les seves instruccions. A sota hi ha el menú per a escollir la opció desitjada. Si per exemple es vol accedir a la número 1, només cal teclejar el número 1 i posteriorment la tecla Enter. Després s'executarà la opció desitjada, i es tornarà a mostrar el menú per a poder seleccionar altres opcions.

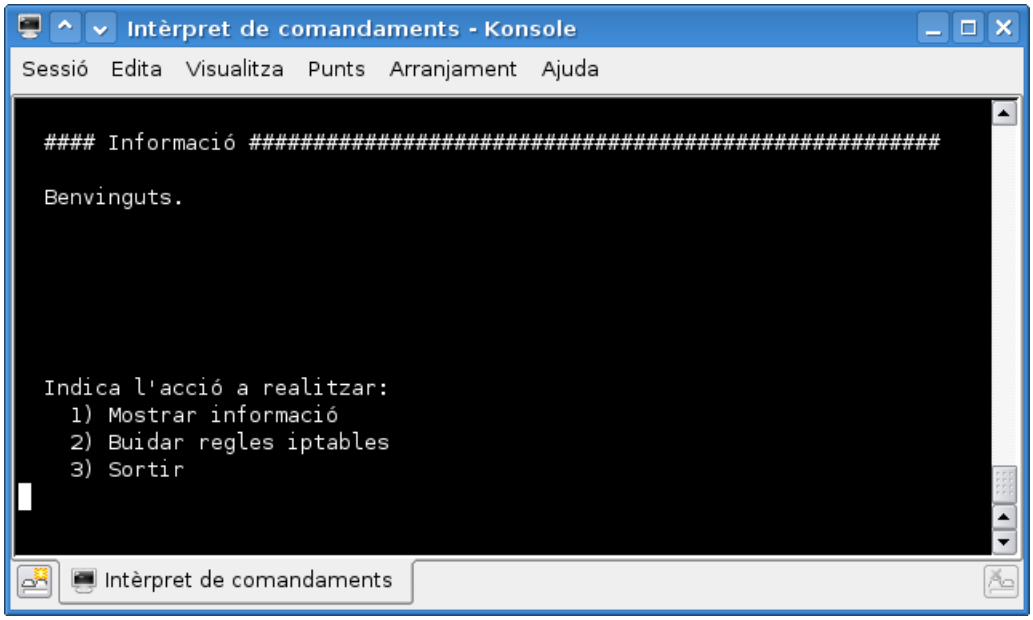

Figura 61: Resetejar regles - Inici

3. Per netejar les regles, cal seleccionar la opció número 2. Un cop executada aquesta opció, ja s'hauran tret totes les regles de l'iptables i es podrà tornar a accedir a l'aplicació remotament.

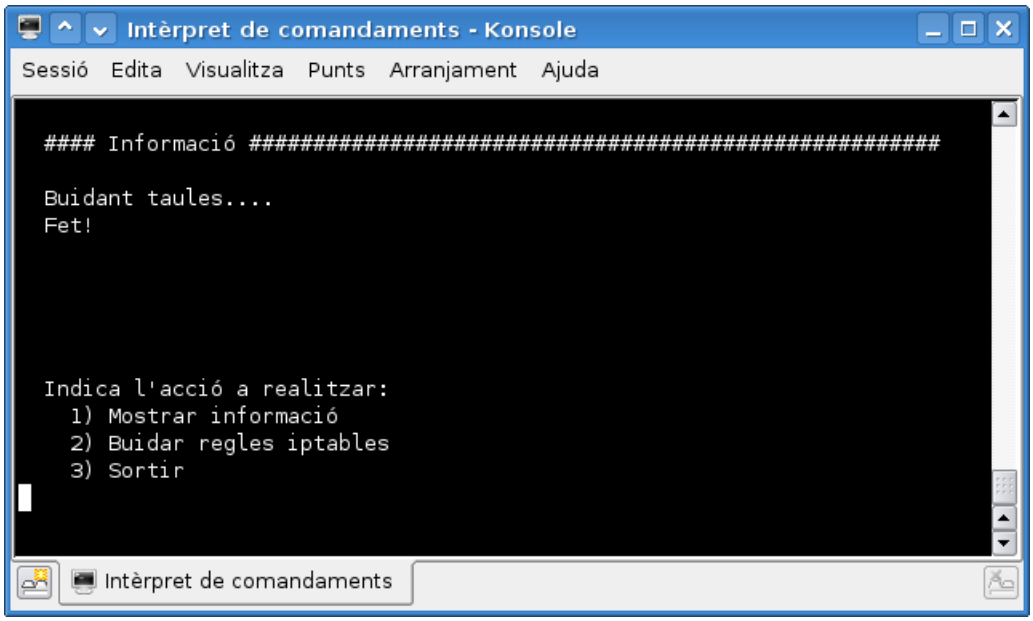

Figura 62: Resetejar regles - Reset

4. Ara només cal sortir de l'aplicació (opció número 3).

C Scripts

C.1 /home/emergency/tool.sh

```
#!/bin/bash

#
# INFO: Script per a resetejar les regles de l'iptables en
# cas d'emergencia.
#

# directori de l'script
export SCRIPT_DIR=`dirname $0`

clear
echo ""
echo "  #### Informació ######################################################"
echo ""
echo "  Benvinguts."
echo ""
echo ""

# bucle
while [ 1 ]; do

        # opcions
        echo ""
        echo ""
        echo ""
        echo ""
        echo "  Indica l'acció a realitzar:"
        echo "    1) Mostrar informació"
        echo "    2) Buidar regles iptables"
        echo "    3) Sortir"
        #echo "Prem el numero desitjat: "
        read case;

        case $case in
                1)
                        # + informacio
                        clear
                        echo ""
                        echo "  #### Informació ######################################################"
                        echo ""
                        echo "  Aquesta utilitat serveix per a buidar les regles de l'iptables en"
                        echo "  cas d'emergència. Per a fer això, cal sel.leccionar la opció 2."
                        echo ""
                        ;;

                2)
                        # buidar regles
                        clear
                        echo ""
                        echo "  #### Informació ######################################################"
                        echo ""
                        echo "  Buidant taules...."
                        /usr/bin/sudo /sbin/iptables-restore < $SCRIPT_DIR/buit.ipt
                        echo "  Fet!"
                        echo ""
                        ;;

                3)
                        # sortir
                        clear
```

Figura 63: Codi de /home/emergency/tool.sh (part 1/2)

```
61                  echo ""
62                  echo "  #### Informació ####################################################"
63                  echo ""
64                  echo "  Sortint..."
65                  echo ""
66                  echo ""
67                  sleep 3
68                  clear
69                  exit
70                  ;;
71
72              *)
73                  # opcio no valida
74                  clear
75                  echo ""
76                  echo "  #### Error ##########################################################"
77                  echo ""
78                  echo "  Opció $case no vàlida."
79                  echo ""
80                  echo ""
81                  ;;
82          esac
83  done
84
85  # EOF
86
```

Figura 64: Codi de /home/emergency/tool.sh (part 2/2)

C.2 /etc/init.d/ipgui-load

```
#!/bin/bash

# script que permet carregar la configuracio del iptables al iniciar el sistema


# variables

# path iptables:
PATHIPT="/sbin/iptables"
# path iptables-restore:
PATHIPTRES="/sbin/iptables-restore"
# arxiu configuracio per defecte:
FILE="/var/www/ipgui/saves/default.ipt"


# script que s'executa al iniciar el sistema
script-start(){
	echo "ipGUI: Carregant la configuració..."

	if [ -e "$FILE" ]
	then
		# si existeix l'arxiu de conf per defecte s'executa
		$PATHIPTRES < $FILE
		echo "ipGUI: Arxiu carregat correctament"
	else
		# si no existeix no es carrega
		echo "ipGUI: No s'ha carregat l'arxiu, $FILE no existeix"
	fi
}


# script que s'executa al aturar el sistema
script-stop(){
	echo "ipGUI: Treient la configuració..."

	$PATHIPT -F
	$PATHIPT -X
	$PATHIPT -P INPUT ACCEPT
	$PATHIPT -P OUTPUT ACCEPT
	$PATHIPT -P FORWARD ACCEPT
	echo "ipGUI: Fet"
}


case "$1" in
  start)
    script-start
    ;;
  stop)
    script-stop
    ;;
  *)
    echo "ipGUI: ERROR, utilització: $0 {start|stop}"
    exit 1
    ;;
esac

exit 0

# EOF

```

Figura 65: Codi de /etc/init.d/ipgui-load

D Captures de pantalla de l'aplicació

Per fer-se una idea de com ha quedat l'aplicació, seguidament es mostraran les captures de pantalla més importants.

Figura 66: Pàgina de login

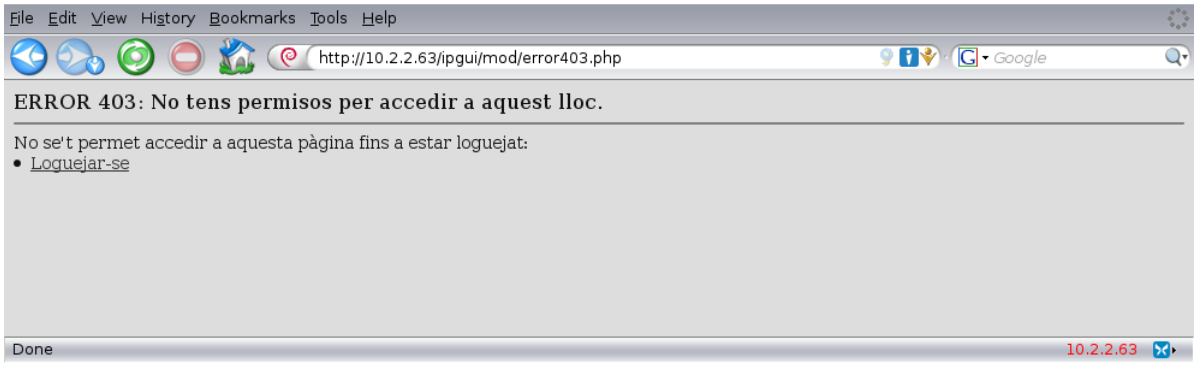

Figura 67: Error de login al intentar accedir a l'aplicació sense estar loguejat

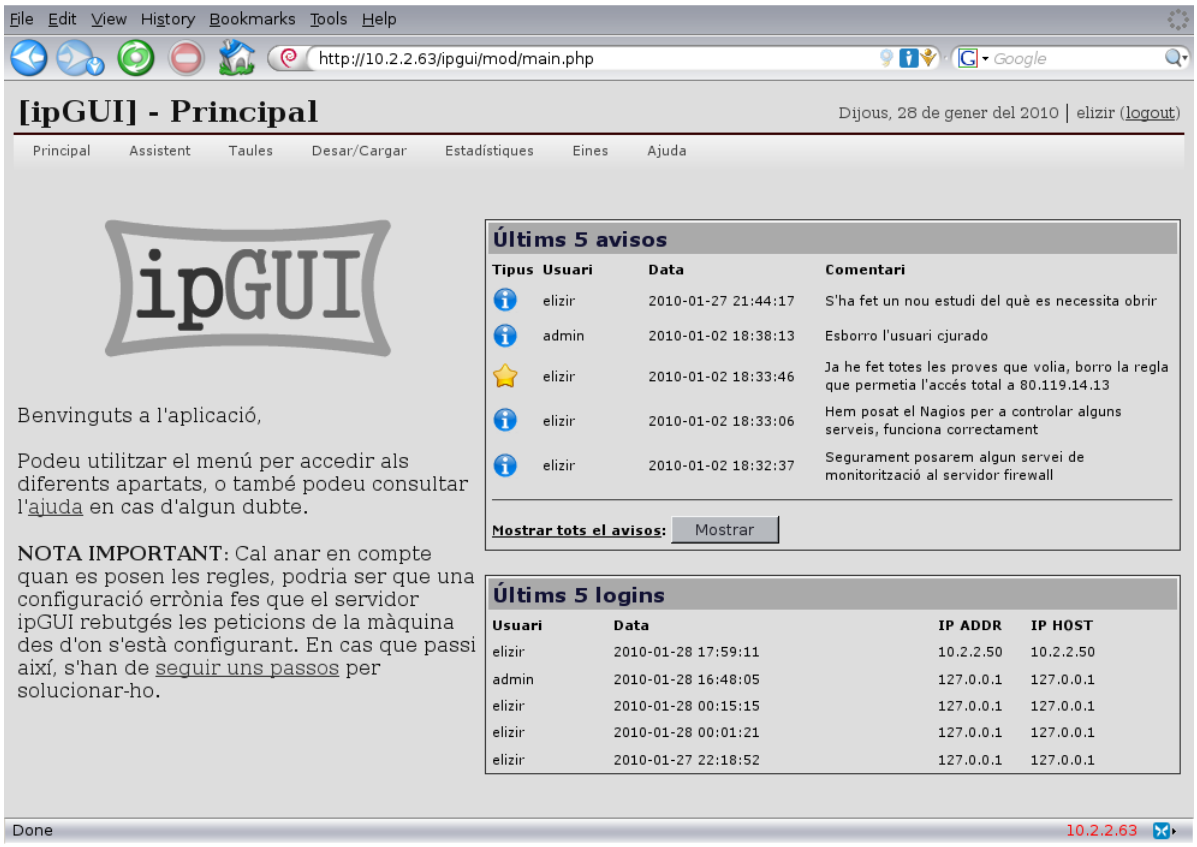

Figura 68: Pàgina principal

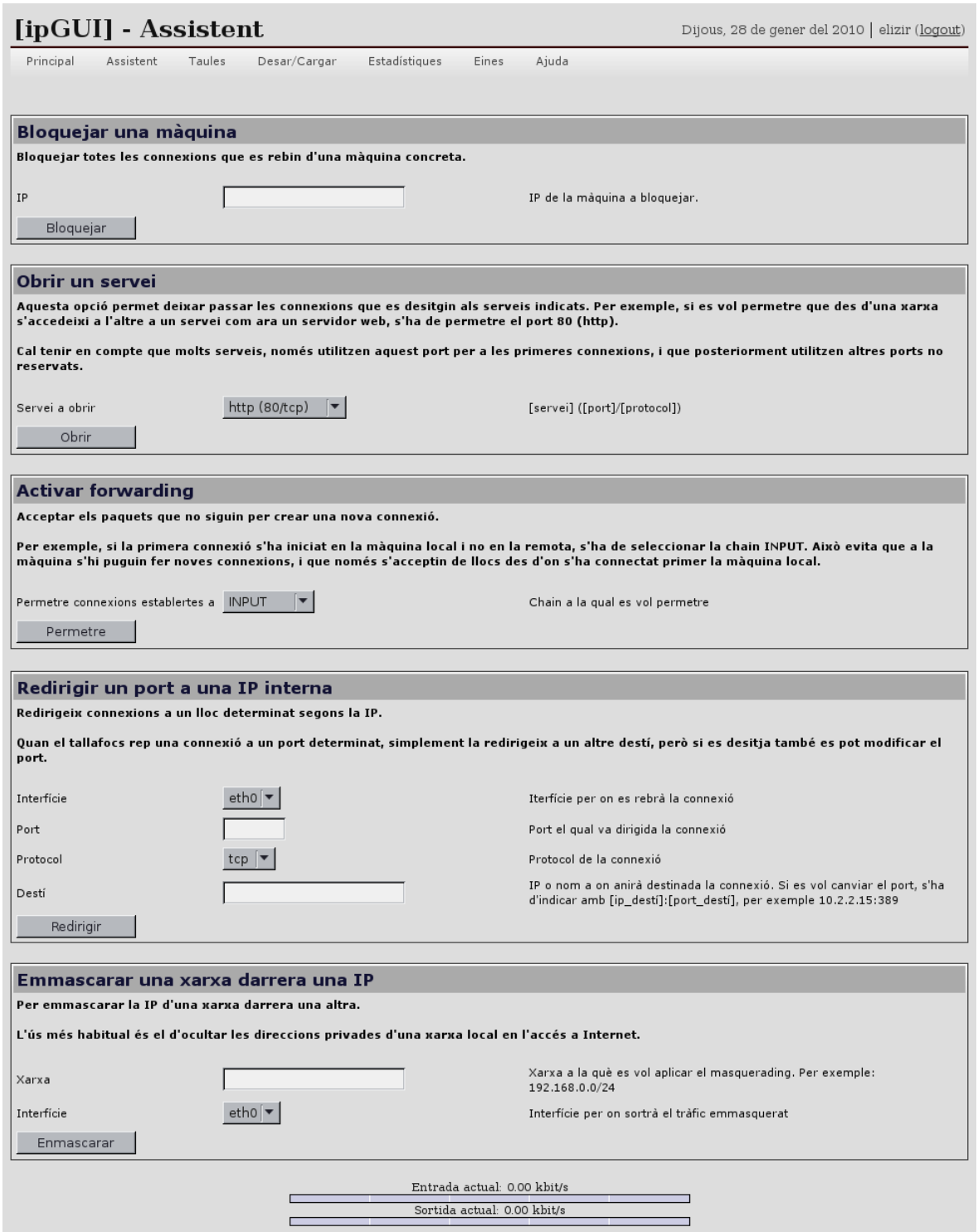

Figura 69: Assistent

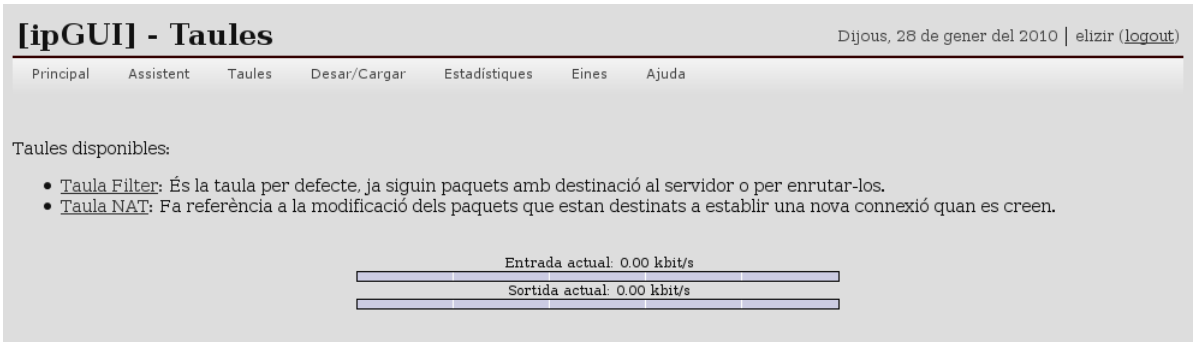

Figura 70: Taules

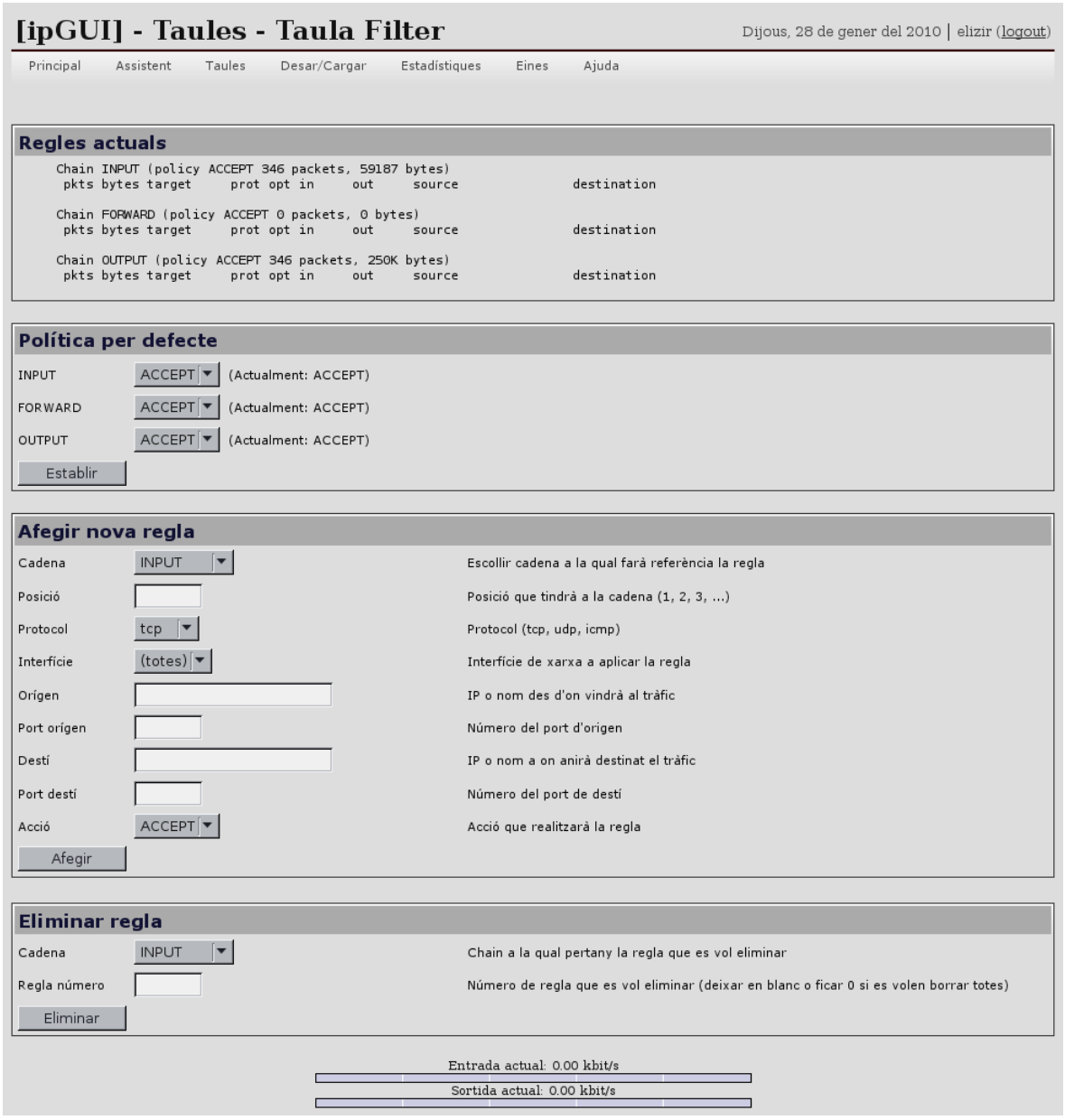

Figura 71: Taula Filter

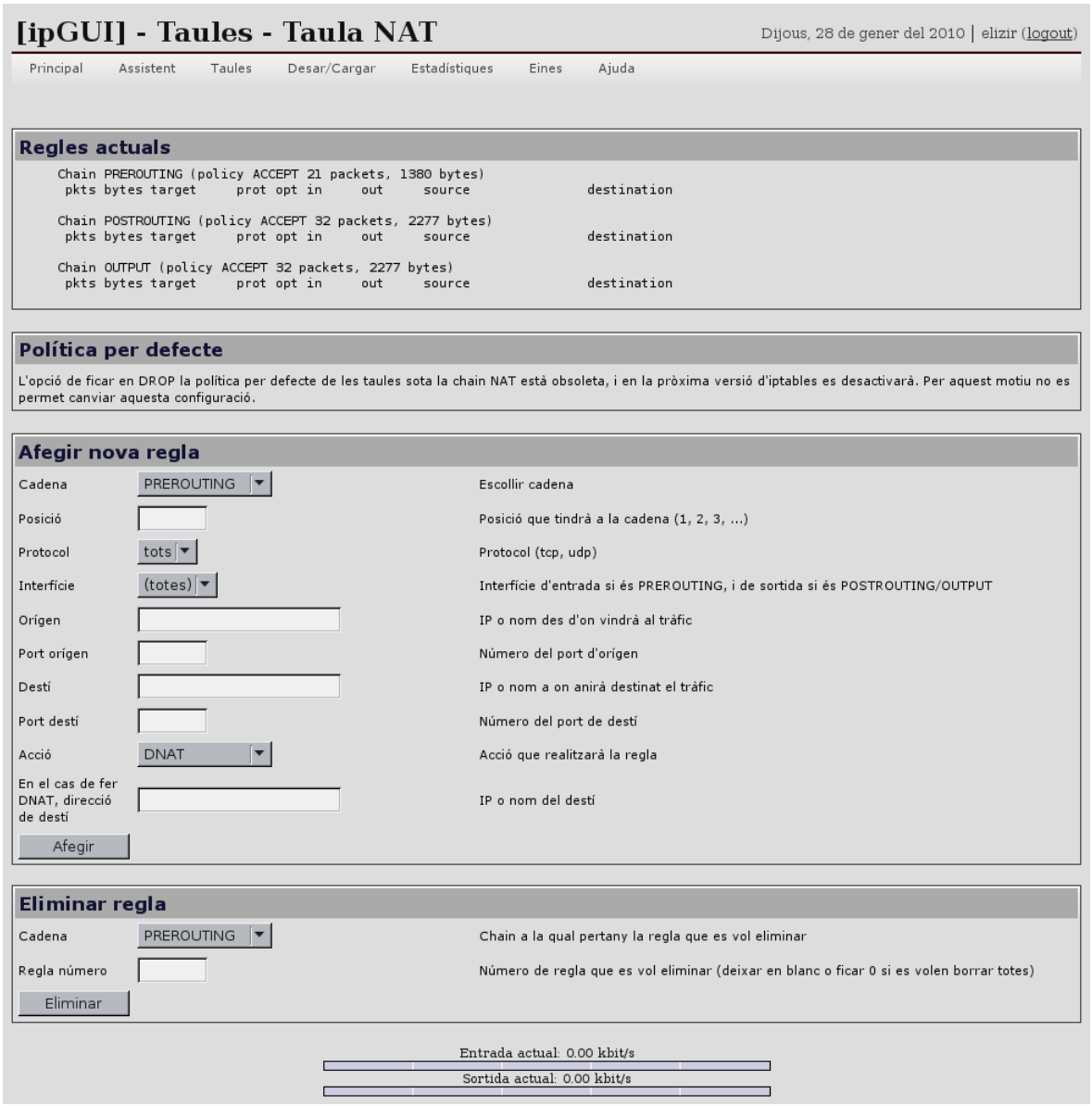

Figura 72: Taula NAT

Figura 73: Desar/Cargar

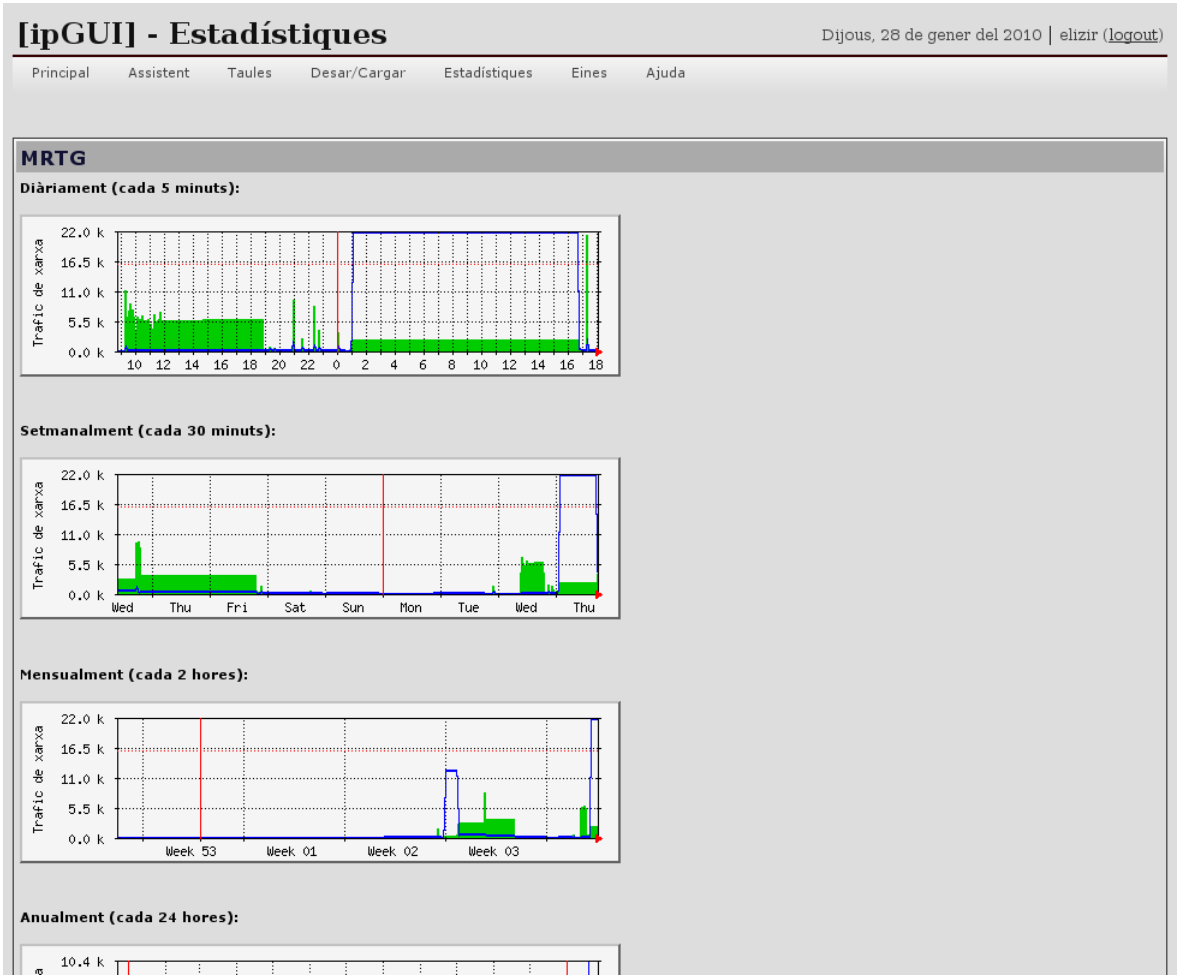

Figura 74: Estadístiques (només part superior)

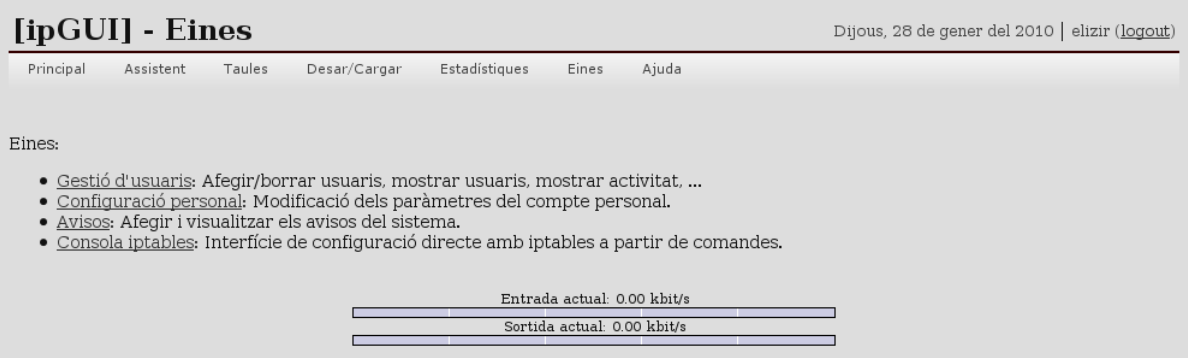

Figura 75: Eines

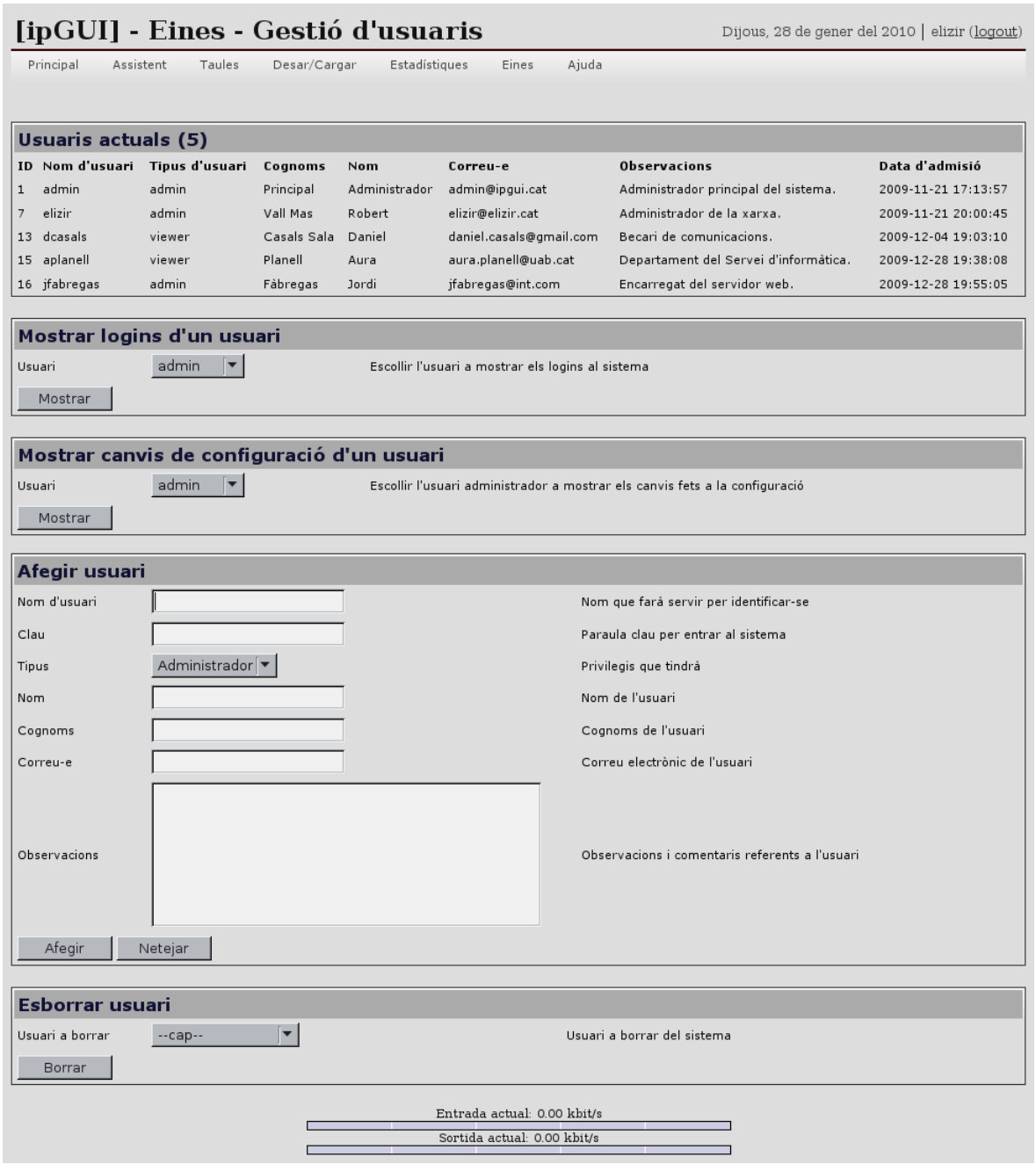

Figura 76: Eines - Gestió d'usuaris

Figura 77: Eines - Gestió d'usuaris - Mostrar logins

Figura 78: Eines - Gestió d'usuaris - Mostrar canvis configuració

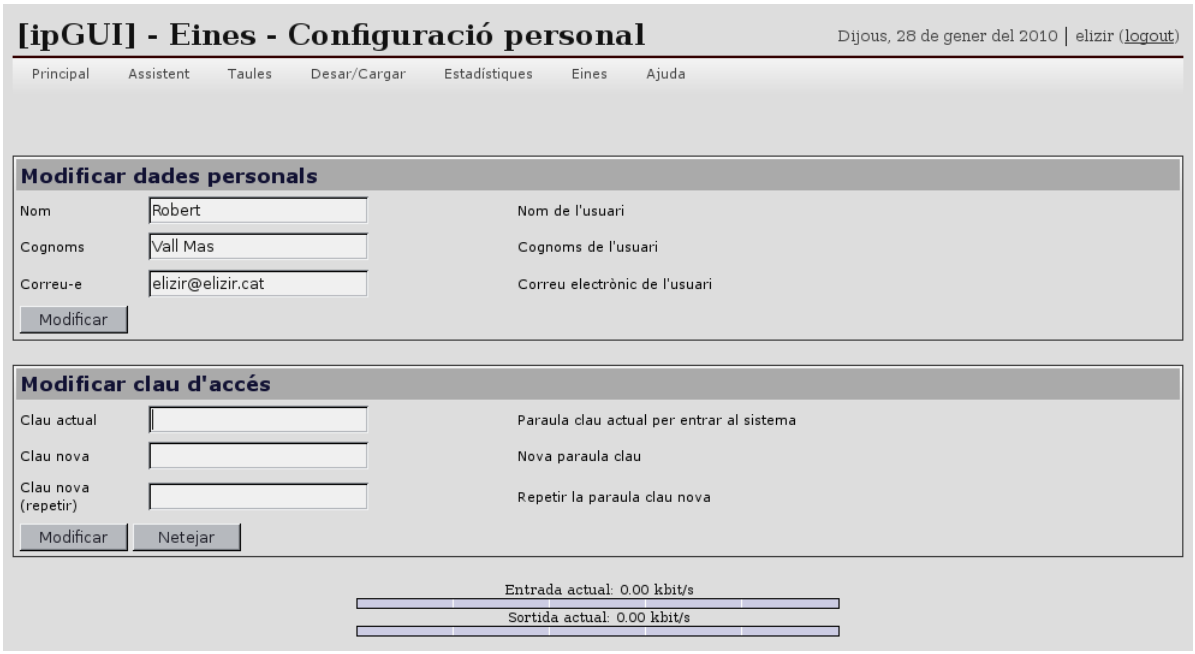

Figura 79: Eines - Configuració personal

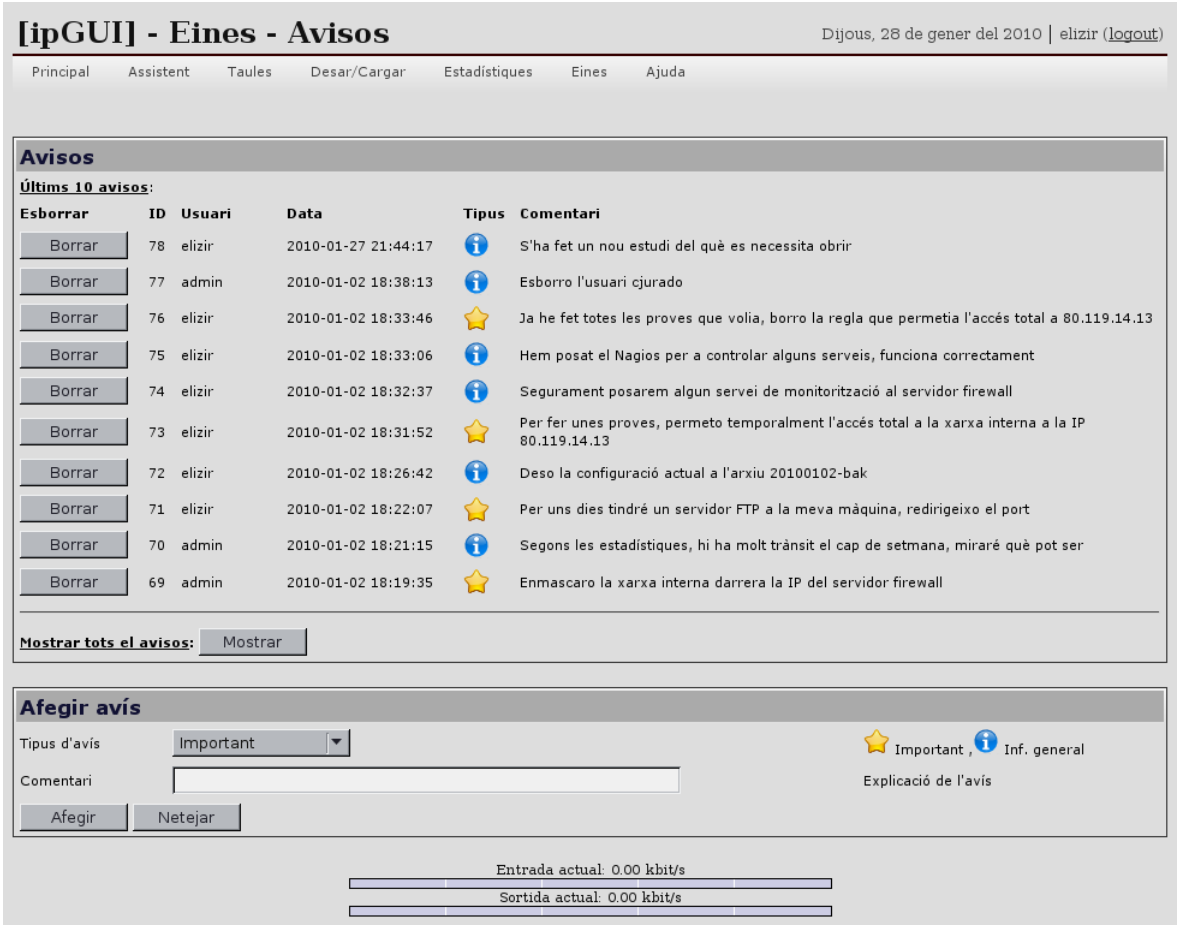

Figura 80: Eines - Avisos

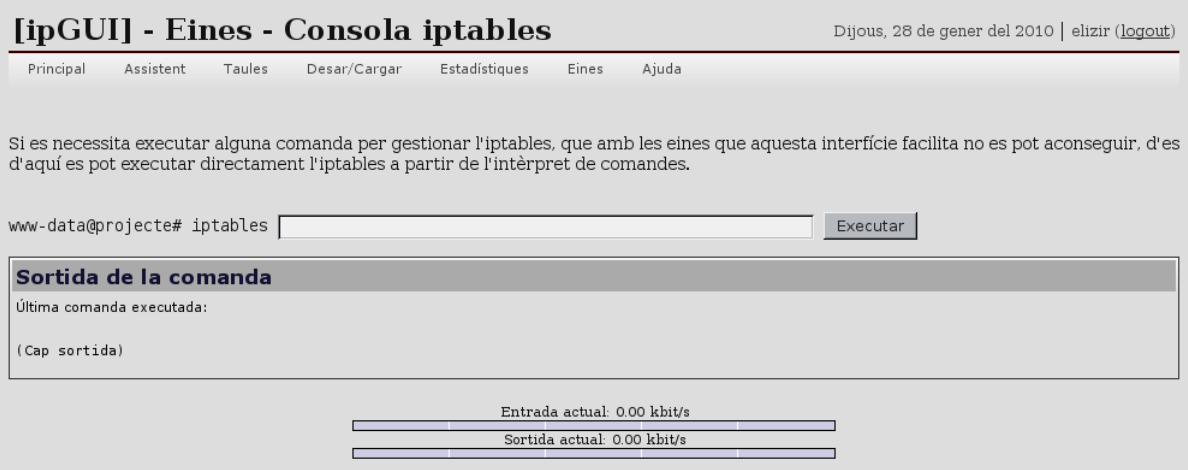

Figura 81: Eines - Consola iptables

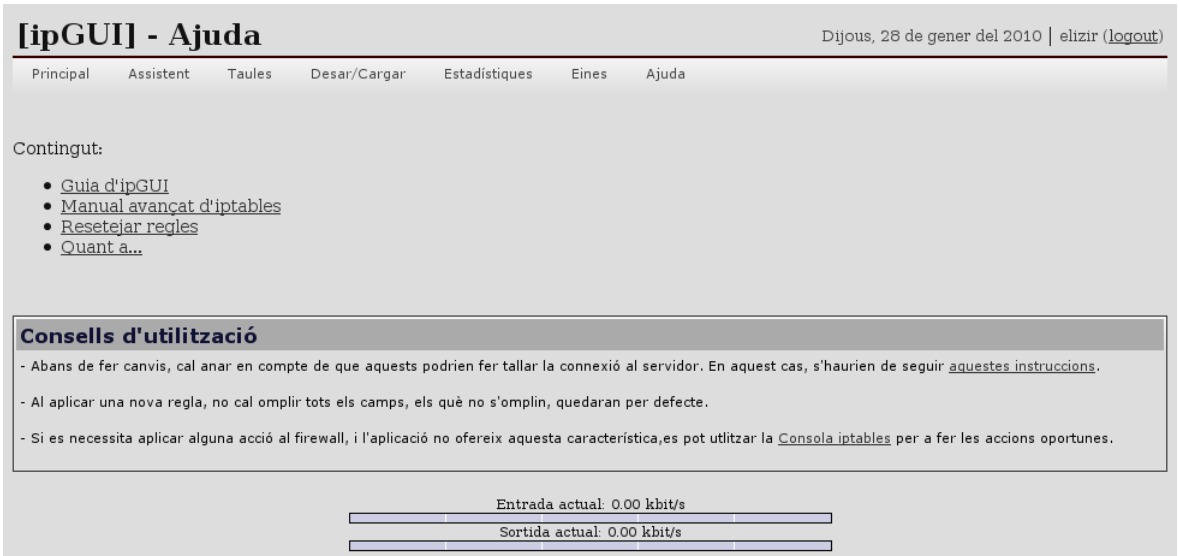

Figura 82: Ajuda

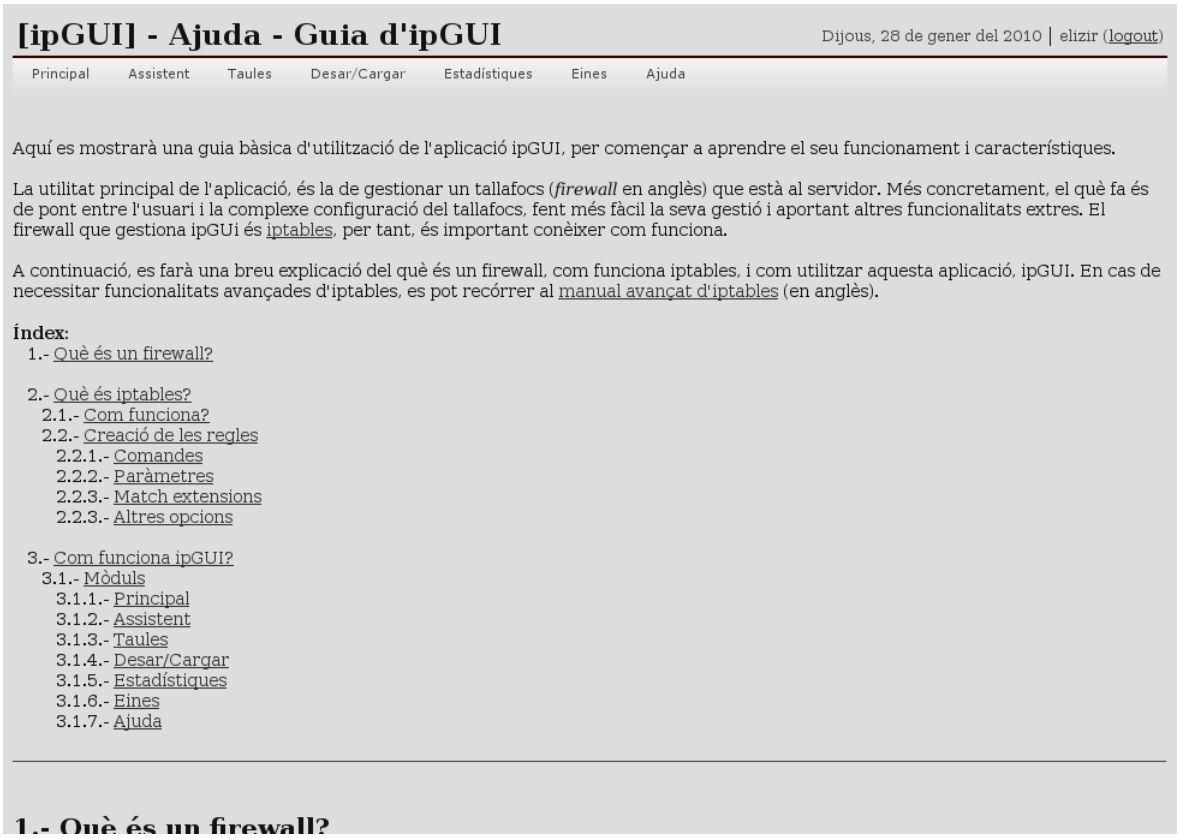

Figura 83: Ajuda - Guia d'ipGUI

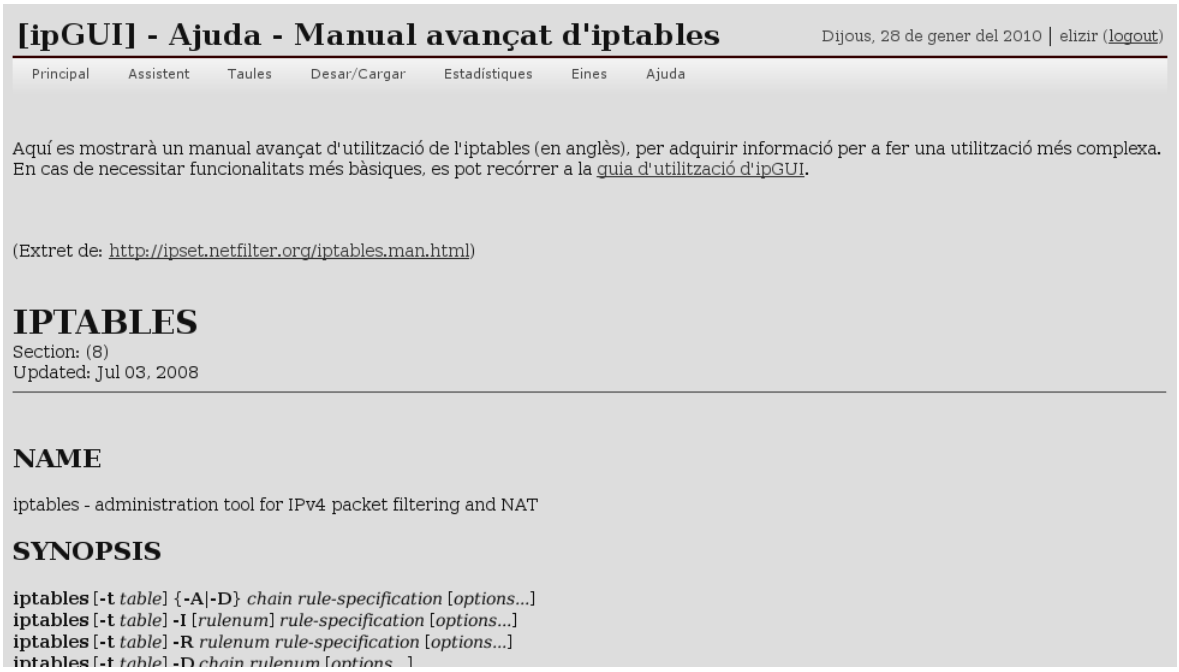

Figura 84: Ajuda - Manual d'iptables

Figura 85: Ajuda - Resetejar regles

Figura 86: Ajuda - Quant a...

Final dels annexes

Agraïments

Al meu tutor de projecte, que m'ha sabut guiar i ha aportat idees al projecte perquè sigués més complet, i també per algun consell que m'ha estalviat molta feina.

A tots els professors de la UAB, altres professors d'estudis anteriors i persones que m'han ensenyat alguna cosa al llarg de la meva vida.

I als meus pares, que a part de moltíssimes altres coses, m'han pagat els estudis els quals espero acabar amb aquest projecte.

Firma de l’autor